(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 999 489 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
10.05.2000 Bulletin 2000/19

(51) Int. Cl.[7]: **G06F 1/00**

(21) Application number: **99203634.3**

(22) Date of filing: **04.11.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **06.11.1998 US 107464 P**
01.11.1999 US 430871

(71) Applicant: **CITIBANK, N.A.**
New York, New York 10043 (US)

(72) Inventors:
- **Teller-Kanzler, Jeri**
  Edison, New Jersey 08820 (US)
- **Dunbar, Thomas**
  Colonia, New Jersey 07067 (US)
- **Katz, Stephen**
  West Hills, New York 11747 (US)

(74) Representative: **Hynell, Magnus**
Hynell Patenttjänst AB,
Patron Carls väg 2
683 40 Hagfors/Uddeholm (SE)

(54) Method and system for evaluating information security

(57) A method and system for evaluating information security and developing an effective information security infrastructure for an entity makes use of an information security evaluation model having, for example, five levels with varying characteristics which explain where the entity stands with regard to threats and vulnerabilities to its information security at any point in time. The evaluation can be performed manually or automatically by a computer program running, on a computer, such as a personal computer and includes, for example, identifying one or more information resources of the entity, receiving information about one or more information security characteristics for the identified resource, categorizing the information security characteristic or characteristics according to a predefined hierarchy of risk levels, and assessing a degree of business risk for the entity based on the categorization.

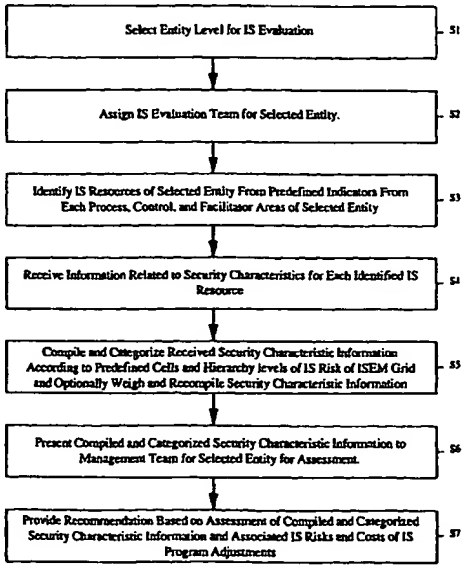


FIG. 6

EP 0 999 489 A2

Description

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Provisional Application No. 60/107,464 filed November 6, 1998.

FIELD OF THE INVENTION

[0002] The present invention relates generally to the field of evaluating information security, and, in particular, to a method and system for evaluating and developing an effective information security infrastructure.

BACKGROUND OF THE INVENTION

[0003] Organizations of all sizes, for example, small businesses, as well as large businesses, are currently at varying levels of security with respect to information systems, such as their computer systems and networks, which present varying levels of business risk in their daily operations. Generally, such organizations have no effective way to determine whether they are information security astute and whether they have the proper programs and services in place to be considered astute regarding the security of their information. Further, even if they have some systems in place to deal with incidents which may compromise the security of their information, they have no effective way to guarantee whether they are in a highly alert state of readiness or simply a mediocre state of readiness if such an incident occurs. Nor do they have an effective way to evaluate whether particular programs which may be in place are in place at the optimum point to deal with such incidents.

[0004] Many of such entities operate under the mistaken assumption that their information is secure or, for example, that an intruder or hacker would not be motivated to try to gain access to their information systems. Likewise, many such entities mistakenly assume that their employees are aware of and in compliance with the entities' requirements for maintaining and working in a secured environment relative to the entities' information systems. Such entities operate under the assumption, but without any assurance, that information relative to their products and services is confidential and will remain confidential. They assume that their level of risk for a security breach is low, when indeed the level of risk of such a breach may be very high. Such unwarranted assumptions themselves create an additional level of business risk.

[0005] Various attempts have been made to address the problems associated with evaluating and developing effective information security infrastructures at different levels of businesses with different levels of sophistication using various levels of technology. Some of such attempts work in some parts of business, and others work on information technologies only. Some are paper-based. However, none have been particularly successful or effective in encompassing, defining, and classifying vulnerabilities, risk, and threats and providing information security infrastructure solutions at all levels of business and technology.

[0006] There is a current need to provide a relatively simple and efficient method and system for evaluating existing information security and for developing an effective information security infrastructure.

SUMMARY OF THE INVENTION

[0007] It is a feature and advantage of the present invention to provide a method and system for evaluating and developing an effective information security infrastructure which defines a set of controls for assessing and compensating for vulnerabilities in each organizational component, such as technology and business processes.

[0008] It is a further feature and advantage of the present invention to provide a method and system for evaluating and developing an information security infrastructure which furnishes a means for defining and classifying the degree of risk associated with information assets, where the risk is defined as the economic value, worth or exposure or the reputational impact of an information asset.

[0009] It is another feature and advantage of the present invention to provide a method and system for evaluating and developing an information security infrastructure which assists an organization in determining the nature of threats or vulnerability to the organization's information systems.

[0010] It is an additional feature and advantage of the present invention to provide a method and system for evaluating and developing an information security infrastructure which affords tools for assessing and analyzing the impact of threats to an organization's information systems and recommends solutions to deal with such threats.

[0011] To achieve the stated and other features, advantages, and objects, an embodiment of the present invention method and system for evaluating information security for an entity which makes use of an information security evaluation model grid having, for example, five different levels with varying characteristics which explain where the entity stands with regard to information security risks at any given time. The method and system for an embodiment of the present invention includes, for example, identifying one or more information security resources related to an information security area of the entity, such as an organizational environment area, a business commitment area, a policy and standards area, and an information security programs and service area of the entity. The identification can be performed either manually or can be received on

a computer program running on a computer, such as a personal computer.

[0012] In the method and system for an embodiment of the present invention, the information resources related to the organizational environment area of the entity relates, for example, to one or more corporate structure resources and responsibility and accountability resources. The business commitment area of the entity relates, for example, to one or more management resources, funding resources, incident management resources, awareness and education resources, operations resources, information ownership resources, and information classification resources. The policy and standards area of the entity relates, for example, to one or more existence and maintenance resources and enforcement and measurement resources. The information security programs and services area of the entity relates, for example, to one or more prevention resources, detection resources, and verification resources.

[0013] In the method and system for an embodiment of the present invention, information is received about one or more information security characteristics for the identified information security resource which is indicative of a pre-defined risk level for the information security of the entity and which also indicates a pre-defined level of readiness of the entity to deal with a risk to the information security of the entity. The pre-defined levels of readiness include, for example, a complacent level of readiness, an acknowledgment level of readiness, an integration level of readiness, a common practice level of readiness, and a continuous improvement level of readiness. Likewise, the information can be gathered and received manually or can be received by entering on the computer program running on a computer, such as a personal computer.

[0014] In the method and system for an embodiment of the present invention, the complacent level of readiness is characterized by a propensity of the entity to resignation to the current information security environment of the entity. The acknowledgment level of readiness is characterized by a propensity of the entity to acknowledgment of a need to improve the information security of the entity. The integration level of readiness is characterized by a propensity of the entity to integrate existing information security programs and services of the entity. The common practice level of readiness is characterized by a propensity of the entity to customarily practice information security procedures for the entity. The continuous improvement level of readiness is characterized by a propensity of the entity to continuously improve information security practices for the entity.

[0015] In the method and system for an embodiment of the present invention, the information security characteristic or characteristics are categorized according to a pre-defined hierarchy of the information security risk levels that are associated with various information security characteristics and which are also indicative of the pre-defined levels of readiness of the entity to deal with a risk to the information security of the entity. Again, the categorization can be performed manually or automatically by the computer program running on the computer, such as a personal computer. Further, the categorized information security characteristic or characteristics can be weighted either manually or automatically by the computer program and recategorized manually or by the computer program.

[0016] In the method and system for an embodiment of the present invention, the categorized or weighted and recategorized information security characteristic or characteristics are used as the basis for an assessment of the degree of business risk for the entity. The assessment can be performed either manually or automatically by the computer program. Another aspect for an embodiment of the present invention includes, for example, selection of the entity for which to evaluate the information security, for example, from a unit level entity, a business level entity, or an organization level entity. A further aspect for an embodiment of the present invention includes, for example, assigning an evaluation team for the selected entity. An additional aspect for an embodiment of the present invention includes, for example, generating a recommendation for a security improvement based at least in part on the assessed degree of business risk and at least in part on the cost of the security improvement.

BRIEF DESCRIPTION OF THE ATTACHMENTS

[0017]

Figs. 1 through 5 show a grid which illustrates an example of five levels of information security for the information security evaluation model for an embodiment of the present invention; and

Fig. 6 is a flow chart which illustrates and example of the process of evaluating the information security infrastructure for an entity using the information security evaluation model grid of Figs. 1 through 5 for an embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0018] Referring now in detail to an embodiment of the present invention, an example of which is illustrated in the accompanying drawings, the system and method for an embodiment of the present invention makes use of an information security evaluation model having, for example, five different levels with varying characteristics which explain where an organization is with regard to threats and vulnerabilities to its information security at any given point in time. The five levels of the ISEM correspond generally to how ready an organization is to deal with an incident, such as an intrusion into the organization's information system by a hacker.

[0019] Figs. 1- 5 show a table or grid 2 which illustrates an example of five levels of information security (IS) for the information security evaluation model (ISEM) for an embodiment of the present invention. Referring to Figs. 1 - 5, the first level 4 of the ISEM grid 2 is complacency, which defines an organization that is contented or resigned to its current environment. The first level 4 characterizes an organization, for example, that is contented, satisfied, or resigned to the current environment. At the first level 4, existing circumstances are accepted with an attitude of "If it's not broken, don't fix it."

[0020] In an embodiment of the present invention, complacency at the first level 4 of the ISEM grid 2 is characterized, for example, in that existing programs and services are perceived as sufficient. Generally, system availability requirements are understood, and failure to provide adequate security is viewed as an 'operations only' issue. Some threats are known, but are not analyzed or understood. Protection is seen as a function of the physical facility, and safeguards are physical network components that are usually installed in an ad hoc manner. Information assets are not considered as separate entities requiring security, and IS is not formal and consists mainly of systems administrators, information systems administrators, or quality assurance and/or compliance units. The requirement for passwords/user identifications may or may not be a commonplace occurrence, and directory set ups of "read," "write," and "share" are known but may not be fully understood. A help desk is used to report incidents with no escalation, and incidents may or may not be resolved. Also, at the first level 4, IS incidents are viewed as "someone else's problem," and IS policies and standards are minimal, and may or may not be documented.

[0021] The consequences to an organization of complacency at the first level 4 of the ISEM grid 2 for an embodiment of the present invention include, for example, no ownership of information or sense of awareness of IS. The organization is not in a state of alertness or readiness, and IS budgets are typically small or nonexistent. Information owners do not exist, and responsibility and/or authorization is lacking. Information is not classified, and there is no relationship to business risk. Security incidents are not reported and tracked as such and are managed as crisis events. In addition, at the first level 4, audit controls and process and procedures are built around complacent characteristics.

[0022] In an embodiment of the present invention, with complacency at the first level 4 of the ISEM grid 2 for an embodiment of the present invention, the response of the organization to an IS incident is reactionary. For example, if someone breaks into the organization's network or server and steals the organization's confidential documentation, a first level 4 or complacent organization initially takes a long time to determine whether such a break-in has indeed occurred. The organization may not be aware of the break-in for an extended period of time. When the organization finally learns of the break-in, it has no mechanism for reporting or responding to the break-in. Such an organization does not usually have any budgeted dollars with which to employ someone to help deal with the break-in, so it has a high impact on the organization. Such a reactionary response to an information security breach is expensive, and usually the organization's management at the first level 4 over-reacts or perhaps becomes panic-stricken.

[0023] Referring further to Figs. 1 - 5, the second level 6 of the ISEM grid 2 for an embodiment of the present invention, is acknowledgment, which is represented by an organization whose management acknowledges that perhaps they need to do something to work in a more secure environment for IS. At the second level 6, change and validation of IS requirements is accepted, and management understands risk as it pertains to IS.

[0024] In an embodiment of the present invention, at the acknowledgment or second level 6 of the ISEM grid 2, some of the business people within the organization realize that there are risks pertaining to the organization's information security and are willing to allocate money to try to avoid such risks. They are also willing to implement at least some monitoring tools or training of at least some of their employees for the purpose. At the second level 6, they are beginning to become more alert to the fact that an information security breach can happen.

[0025] Characteristics of the acknowledgment or second level 6 of the ISEM grid 2 for an embodiment of the present invention include, for example, a realization that a "silo" approach will not work, that a focused IS program and IS organization is required, and that existing IS processes are fragmented. Additional characteristics of acknowledgment at the second level 6 include, for example a realization that information assets must be owned in a concept of "information ownership" and that information must be "classified" as a function of risk to the business unit.

[0026] Other characteristics of the acknowledgment or second level 6 of the ISEM grid 2 for an embodiment of the present invention include, for example, that management is willing to allocate funds for IS products and systems, which is usually operations oriented at this level. Management also realizes that IS is needed, and a corporate IS officer has been assigned or is being considered. While IS professionals are assigned, they are usually operations staff at this level. Incidents are still reported through a help desk, but escalations are refocused. IS organizations receive reports of incidents from the help desk as a function of the escalation chain. At the second level 6, some response teams are being built within the business units and the IS organization, and reporting of business level IS activities to senior management exists but is sporadic.

[0027] The results for an entity at the acknowledgment or second level 6 of the ISEM grid 2 for an embodiment of the present invention include, for example, that "silos" particular to IS between groups begin to diminish. IS requirements are mandated, but process and programs to manage them are not yet built. Ad hoc requests for IS status is made by management to line managers, pressure to make business managers more accountable for IS comes from the top, down, and IS topics begin to appear on management meeting agendas. In addition, at the second level 6, accountability for information assets may be assigned to a person, and the level or protection required for information assets is considered when making decisions.

[0028] Other results for an entity at the acknowledgment or second level 6 of the ISEM grid 2 for an embodiment of the present invention include, for example, that budgeted dollars are spent on high priced security technologies, which are usually data center centric. The blame for incidents, system failures, or availability shifts between operations and information security providers, and attention to incident management increases. Additionally, at the second level 6, end user productivity can be effected by IS safeguards mandated to protect corporate assets, and the organization begins to move towards an alert state, although it is not yet in a readiness state.

[0029] Referring still further to Figs. 1- 5, the third level 8 of the ISEM grid 2 for an embodiment of the present invention is integration, in which an organization's management takes any existing programs and services that are already in the organization and integrates them or penetrates them down into all levels of the business so they work in concert together. In an organization at the third level 8, IS requirements across corporate boundaries are accepted, and threats and vulnerabilities are understood, as well as a requirement for cross functionality.

[0030] At the integration or third level 8 of the ISEM grid 8, for an embodiment of the present invention, there is a state of readiness, because information security requirements are integrated between the levels and the businesses, and people know what to do and how to respond to an information security breach. For example, when an incident occurs, they know not to publicize it, because publicity can cause damage to the organization's reputation. At the third level 8, they know to report the incident to the appropriate security officer, which has been designated beforehand.

[0031] Characteristics of an organization at the integration or third level 8 of the ISEM grid 2 for an embodiment of the present invention include, for example, that management realizes that IS adds value to the organization, and there is a general acceptance of an organization-wide, standards based, IS infrastructure. An IS infrastructure is designed to penetrate all business entities and levels, and a centralized corporation IS office or officer is established, funded, and staffed, and granted authority over IS matters. Senior level information owners with responsibility are identified, and information assets are assigned sponsors with authority at the business, customer, and/or user level. At the third level 8, information has been and/or is being classified based on business risk, and an organization-wide process relationship exists for reporting incidents.

[0032] Other characteristics of an organization at the integration or third level 8 of the ISEM grid 2 for an embodiment of the present invention include, for example, that organization-wide process relationships exist for responding to incidents, for disseminating security alerts or threat management, and for certifying security products. Virus reporting is centralized, and a security building permit process is part of the application/product development lifecycle. A process relationship exists between the security incident response teams, business incident response teams, and organization fraud entities, and IS vulnerability assessment tools are made available to the business units. At the third level 8, all new hire packages include an IS package and training schedule, IS training programs are available, and IS metrics are collected, analyzed, and used to make decisions.

[0033] The results for an entity at the integration or third level 8 of the ISEM grid 2 for an embodiment of the present invention include, for example, that products/applications are delivered with appropriate levels of security, end users can more readily identify reportable incidents, and mutually beneficial process relationships exist between the business units. IS metrics are used for decision making, trending, and threat management, IS becomes process driven, and IS is managed vertically from the top, down and horizontally or cross "silo." IS programs and services are being designed to meet corporate requirements, IS practices are mandated, and accountability for information assets are assigned to the "right people." IS vulnerability assessments are being incorporated in the business unit's self-assessment process, information assets are being classified as a function of risk, and information ownership is omnipresent. The organization at the third level 8 is in an alert state and is moving towards a readiness state.

[0034] Referring again to Figs. 1 - 5, the fourth level 10 of the ISEM grid 2 for an embodiment of the present invention is common practice, which means that there has been a culture switch within the organization and that providing IS programs and services is a common practice of the organization. For example, it becomes a common practice for employees to password their workstations, to turn their equipment off at night, to take IS precautions when traveling, to lock away confidential documentation. Off-site storage is provided for confidential documentation. At the third level 10, such IS actions become common practice. Employees think about IS at all times. In an organization at the third level 10, IS requirements reach the business entity level as daily business procedures, IS practices are widespread

throughout the corporation, and IS practices become an habitual occurrence.

[0035] In an organization at the fourth level 10 of the ISEM grid 2 for an embodiment of the present invention, information security is a common practice. People know what to do and money is budgeted for information security. Information security is a part of building the organization's applications and products. The common practice characteristics of an organization at the fourth level 10 include, for example, that the integration of IS programs and services with the business unit's is complete. Management actively and visibly participates in the IS programs and services, the IS infrastructure is established, IS policy and standards are established, understood, and implemented, and the practice of IS is considered daily.

[0036] In an organization at the fourth level 10 of the ISEM grid for an embodiment of the present invention, information classifications are based on business risk analysis, incident reporting is centralized and focused, business incident response teams are built, and a process relationship exists between the business incident response teams and a security incident response team. Virus incidents are tracked and reported, IS metrics are available at the business level, and business level IS officer resource allocation is optimized. At the fourth level 10, IS product certification is ongoing, and management meetings include IS awareness agenda items.

[0037] The results for an organization at the common practice or fourth level 10 of the ISEM grid 2 for an embodiment of the present invention include, for example, that IS is a common business practice, and there is consistency in IS products. IS programs and services are interactive, there is routine corporate wide IS reporting, and mutually beneficial relationships exist between the organizational units. There is consistency in corporate IS initiatives, IS programs and services reflect the organization's environment, the organization understands its vulnerabilities, and virus incident trending, tracking, and reporting is available. At the fourth level 10, the organization is in an alert state, as well as a readiness state.

[0038] Referring once again to Figs. 1 - 5, the final or fifth level 12 of the ISEM grid 2 for an embodiment of the present invention is continuous improvement, in which an organization for which IS culture has become a common practice, looks continually at technologies for improving the security of information, and works with those technologies to continuously improve the IS environment within the organization. In an organization at the fifth level 12, IS practices are a proven corporate benefit and quality state with a corresponding increase in productivity and value, and IS becomes a part of the brand.

[0039] In an embodiment of the present invention, at the continuous improvement or fifth level 12, the organization is in a highly alert state with regard to IS and ready to deal with any incident, such as a hacker. When such an incident occurs, response teams are ready to go into place and resolve the problem. An organization that is at the fifth level 12 continuously monitors the threats to its IS out in the marketplace and is able to evaluate how the threats affect the organization and then make changes based on those threats. Such an organization looks at more cost-effective alternatives than what it currently has in place. The organization frequently re-classifies its information based on various risks. It changes its policies and standards to reflect changes in technology or changes in its classification of information. An organization at the fifth level 12 does such things relatively quickly. Implementation cycles are designated in Web years, which is usually about three months. At the fifth level 12, IS activities are encouraged in the organization.

[0040] An organization at the fifth level 12 of the ISEM grid 2 for an embodiment of the present invention has IS programs and services that are planned and routine. IS is something that happens as part of the planning and strategic planning processes of the organization. The products that emanate from an organization that reaches the continuous improvement or fifth level 12 are trusted products, and buyers of such products know the products can be trusted. IS is considered part of the organization and becomes part of the culture of the organization. In an organization at the fifth level 12, IS is something that people within the organization deal with every day, and knowledge that the organization gains is shared throughout the organization.

[0041] In an organization at the fifth level 12 of the ISEM grid 2 for an embodiment of the present invention, IS program and service initiatives are at a much higher level and function across organizational lines. In the event of an IS incident, the response is quick, and everyone knows what to do, which usually results in savings of money to the organization. There is a mechanism in place for reporting incidents back to management. An organization at the fifth level 12 is constantly alert to information security risks, and the organization is ready to handle such risks, which minimizes losses.

[0042] Characteristics of an organization at the continuous improvement or fifth level 12 for an embodiment of the present invention include, for example, continual reevaluation of threats based on changing threat population and security incidents, and additional or more cost effective alternatives are continually identified. Information classification is continually reviewed for optimal risk/security benefits, IS policies and standards are continually reviewed for completeness and applicability, and implementation cycles are in Web years. IS technical research activities are encouraged to be consistent with rapidly changing environments, IS programs and services are planned, budgeted, and routine for security economics, and the organization is known for providing trusted products. In an organization at the fifth level 12, IS is considered an integral component of the

organization's internal controls, the practice of IS is considered a component of the corporate culture and is second nature, and knowledge is shared.

[0043] The results of the continuous improvement or fifth level 12 of the ISEM grid 2 for an embodiment of the present invention include, for example, that IS process improvement is continuous through program and service initiatives, cross level and cross functional participation, and the sharing of knowledge. Incidents are responded to with corrective actions, feedback to management is consistent, prevention strategies are implemented and continuously improved. Recovery costs are contained, and losses are minimized and anticipated. An organization at the fifth level 12 is in alert state, as well as a readiness state.

[0044] Referring still again to Figs. 1 - 5, the ISEM for an embodiment of the present invention makes use of the grid 2, which includes the five levels of the ISEM, as well as associated process, control and facilitator indicator areas 14. The process, control, and facilitator indicator areas 14 include, for example, organizational environment 16, business commitment 18, policy and standards 20, and IS programs and services 22. The process and control area facilitators and indicators 14, such as organizational environment 16, are the features that determine the results, i.e., make each thing happen, or indicate who determines the status or where each characteristic is at any particular time.

[0045] In an embodiment of the present invention, the process, control, and facilitator indicator areas 14 of the ISEM grid 2 are areas within an organization that have some type of responsibility for information security. Within each process, control and facilitator indicator area 14 there is a definition. For example, organizational environment 16 relates to corporate structure 24 and responsibility and accountability 26. Business commitment 18 relates to management 28, funding 30, incident management 32, awareness and education 34, operations 36, information ownership 38, and information classification 40. Policy and standards 20 relates to maintenance 42 and enforcement and measurement 44. IS procedures and services 22 relates to prevention 46, detection 48, and verification 50.

[0046] Each of the five levels of the ISEM grid 2 for an embodiment of the present invention is documented and within each cell of the grid 2. For example, corporate structure 24 at the first level 4 addresses existing programs and services that are perceived as sufficient and exist in silos, information security that is informal and consists mainly of systems administrators, the absence of a focused IS program or a relationship between business units and IS entities, and the absence of a readiness or an alert state of IS. For another example, responsibility and accountability 26 at the first level 4 addresses the absence of an IS office or officer, the absence of ownership of IS, the view of failure to provide adequate IS as only an operations or technology issue, and the view of IS incidents as someone else's problem.

[0047] In an embodiment of the present invention, the ISEM grid 2 for an embodiment of the present invention takes all of the characteristics and puts them into the proper cell for the analysis and evaluation of the IS of an organization and does it for each process area within the organization. The ISEM grid 2 for an embodiment of the present invention can be used with a tool set on a qualitative basis without weighting, but weighting can serve to quantitatively define or refine the process somewhat.

[0048] In a weighting aspect of an embodiment of the present invention, the ISEM grid 2 is used to weight and score information security by viewing each characteristic within a cell and weighting it as to its importance in the particular level and computing a score. An organization cannot graduate from one level to the next level until it reaches a certain score. The weighting process is an aspect of the present invention, and the calculation of the level of IS is consistent, regardless of the particular tool set that is used to evaluate the cells or evaluate their levels by using, for example, a decision tree or a cumulative process. A tool set is used by an organization to determine the particular level at which the organization stands. The characteristics within each level of the model can be weighted and the results scored using the tool set to identify the level at which the organization stands.

[0049] In an embodiment of the present invention, the resulting score is used by business managers within the organization to make a decision with regard to whether they are satisfied with the particular level at which the organization stands in respect to IS in light of the risk to the business of the organization. If the business managers within the organization find the business risk unacceptable, they can elect to determine, for example, the technology steps necessary to be taken to move to a higher level on the ISEM grid 2 and the costs associated with such steps. If the business risk justifies the costs, appropriate procedures can be implemented to move to a higher level on the ISEM grid 2.

[0050] Fig. 6 is a flow chart which illustrates an example of the process of evaluating an entity's IS infrastructure using the ISEM grid 2 for an embodiment of the present invention. Referring to Fig. 6, at S1, a selection is made for the particular entity for which IS to be evaluated. The selected entity can be, for example, a unit level, a business level or the organization level. At S2, an ISEM certified evaluation team is assigned. At S3, the IS resources of the selected entity are identified from pre-defined indicators, for example, from each process, control, and facilitator indicator area of the entity, such as organizational environment 16, business commitment 18, policy and standards 20, and IS programs and services 22.

[0051] Referring further to Fig. 6, at S4, information is received that relates to security characteristics, for example, for each identified IS resource. For example,

questions concerning the security characteristics of each identified IS resource are considered and answered, which relate to the levels on the ISEM grid 2 and where the entity stands on the ISEM grid 2. For the organization to be, for example, at the first level 4, it must meet certain criteria.

[0052] In order to get to the security characteristics, for example, for the first level 4 of the ISEM grid 2 for an embodiment of the present invention, it is necessary to pose and answer questions about the identified IS resources, such as whether existing IS programs are perceived as sufficient, whether IS is informal and consists mainly of systems administrators, whether a focused IS program exists, whether a relationship exists between business units and IS entities, whether an IS office or officer exists, and the like. The questions can be posed in any number of ways to get to the security characteristics, and the yes or no answers to the questions provide the information that determines the level on the ISEM grid 2 at which the entity stands.

[0053] Referring again to Fig. 6, at 85, the information about the IS characteristics of the entity is compiled and categorized according to a predefined hierarchy of IS characteristics, such as the five levels of the ISEM grid 2. While the compilation and categorization of the IS characteristics can be performed manually, an aspect of an embodiment of the present invention makes use of a computer software application or program referred to as the ISEM tool set or tool kit running, for example, on a personal computer (PC). The ISEM tool kit is used to perform evaluations by the automated software application by process, control, and facilitator indicator area 14. The ISEM tool kit automatically compiles and categorizes the results for each cell of the ISEM grid 2.

[0054] In an additional aspect for an embodiment of the present invention, after posing and answering all of the questions, at S5, the ISEM tool kit optionally performs weighting, recompiles the weighted results, and automatically determines the level within the ISIM grid 2 where the entity stands. The ISEM tool optionally compiles, enters and weights the results. At S6, the compiled and categorized results are presented to a management team for the entity, which assesses the results to determine whether, for example, the entity, is operating at a level on the ISEM grid 2 which meets the entity's IS needs, based on business determined risks. At S7, a recommendation is made by the management team, based on its assessment of the compiled and categorized results according to the ISEM grid 2 and the costs of IS program adjustments, if applicable.

[0055] An embodiment of the present invention identifies threats and vulnerabilities or the risk state of an organization's information and enables the organization to develop an effective IS infrastructure. An embodiment of the present invention defines a set of controls for assessing and compensating for vulnerabilities in each organizational component, such as technology, business process, and the like. An embodiment of the present invention also provides a means for defining and classifying the degree of risk associated with information assets, where risk is defined as the economic value or degree of worth of an information asset and/or the economic exposure and/or reputational impact to the organization. Further, an embodiment of the present invention assists the organization in determining the nature of threats and exploiting vulnerabilities, provides tools for impact assessment and analysis, and recommends solutions.

[0056] Although the invention has been described with reference to these preferred embodiments, other embodiments can achieve the same results. Various modifications of the present invention will be apparent to one skilled in the art, and the above disclosure is intended to cover all such modifications. Accordingly, the invention is limited only by the following claims.

Claims

1. A method for evaluating information security for an entity, comprising:

   identifying at least one information security resource related to an information security area of the entity selected from a group consisting of an organizational environment area, a business commitment area, a policy and standards area, and an information security programs and services area of the entity;
   receiving information about at least one information security characteristic for the identified information security resource;
   categorizing the information security characteristic according to a pre-defined hierarchy of information security risk levels associated with information security characteristics; and
   assessing a degree of business risk for the entity based on the categorization of the information security characteristic.

2. The method of claim 1, wherein identifying the information security resource further comprises identifying the information security resource from one of a corporate structure resource and a responsibility and accountability resource related to the organizational environment area of the entity.

3. The method of claim 1, wherein identifying the information security resource further comprises identifying the information security resource selected from a group consisting of a management resource, a funding resource, an incident management resource, an awareness and education resource, an operations resource, an information ownership resource, and an information classification resource related to the business commitment area of the entity.

4. The method of claim 1, wherein identifying the information security resource further comprises identifying the information security resource from one of an existence and maintenance resource and an enforcement and measurement resource related to the policy and standards area of the entity.

5. The method of claim 1, wherein identifying the information security resource further comprises identifying the information security resource selected from a group consisting of a prevention resource, a detection resource, and a verification resource related to the information security programs and services area of the entity.

6. The method of claim 1, wherein identifying the information security resource further comprises receiving a selection of the identified information security resource on a computer program.

7. The method of claim 1, wherein receiving the information further comprises receiving the information about the security characteristic for the identified information security resource which is indicative of a pre-defined risk level for the information security of the entity.

8. The method of claim 7, wherein receiving the information indicative of the pre-defined risk level further comprises receiving the information indicative of a pre-defined level of readiness of the entity to deal with a risk to the information security of the entity selected from a group consisting of a complacent level of readiness, an acknowledgment level of readiness, an integration level of readiness, a common practice level of readiness, and a continuous improvement level of readiness of the entity.

9. The method of claim 8, wherein receiving the information indicative of the pre-defined level of readiness further comprises receiving the information indicative of the complacent level of readiness which indicates a propensity of the entity to resignation to a current information security environment of the entity.

10. The method of claim 8, wherein receiving the information indicative of the pre-defined level of readiness further comprises receiving the information indicative of the acknowledgment level of readiness which indicates a propensity of the entity to acknowledgment of a need to improve the information security of the entity.

11. The method of claim 8, wherein receiving the information indicative of the pre-defined level of readiness further comprises receiving the information indicative of the integration level of readiness which indicates a propensity of the entity to integrate existing information security programs and services of the entity.

12. The method of claim 8, wherein receiving the information indicative of the pre-defined level of readiness further comprises receiving the information indicative of the common practice level of readiness which indicates a propensity of the entity to customarily practice information security procedures for the entity.

13. The method of claim 8, wherein receiving the information indicative of the pre-defined level of readiness further comprises receiving the information indicative of the continuous improvement level of readiness indicative of a propensity of the entity to continuously improve information security practices for the entity.

14. The method of claim 1, wherein receiving the information further comprises receiving the information at a computer.

15. The method of claim 1, wherein categorizing the information security characteristic further comprises categorizing the information security characteristic according to a pre-defined risk level for the information security of the entity.

16. The method of claim 15, wherein categorizing the information security characteristic according to the pre-defined risk level further comprises categorizing the information security characteristic according to a pre-defined level of readiness of the entity to deal with a risk to the information security of the entity selected from a group consisting of a complacent level of readiness, an acknowledgment level of readiness, an integration level of readiness, a common practice level of readiness, and a continuous improvement level of readiness.

17. The method of claim 16, wherein categorizing the information security characteristic according to the pre-defined level of readiness further comprises categorizing the information security characteristic according to the complacent level of readiness indicative of a propensity of the entity to resignation to a current information security environment of the entity.

18. The method of claim 16, wherein categorizing the information security characteristic according to the pre-defined level of readiness further comprises categorizing the information security characteristic according to the acknowledgment level of readiness indicative of a propensity of the entity to acknowledge a need to improve the information

security of the entity.

19. The method of claim 16, wherein categorizing the information security characteristic according to the pre-defined level of readiness further comprises categorizing the information security characteristic according to the integration degree of readiness indicative of a propensity of the entity to integrate existing information security programs and services of the entity.

20. The method of claim 16, wherein categorizing the information security characteristic according to the pre-defined level of readiness further comprises categorizing the information security characteristic according to the common practice level of readiness indicative of a predisposition of the entity to customarily practice information security procedures for the entity.

21. The method of claim 16, wherein categorizing the information security characteristic according to the pre-defined level of readiness further comprises categorizing the information security characteristic according to the continuous improvement level of readiness indicative of a propensity of the entity to continuously improve information security practices for the entity.

22. The method of claim 1, wherein categorizing the information security characteristic further comprises categorizing the information security characteristic by a computer program.

23. The method of claim 22, wherein categorizing the information security characteristic further comprises weighting the categorized information security characteristic.

24. The method of claim 23. wherein weighting the categorized information security characteristic further comprises automatically weighting the categorized information security characteristic by a computer program.

25. The method of claim 24, wherein weighting the categorized information security characteristic further comprise recategorizing the weighted information security characteristic.

26. The method of claim 25, wherein recategorizing the weighted information security characteristic further comprises automatically recategorizing the weighted information security characteristic by a computer program.

27. The method of claim 1, wherein assessing the degree of business risk further comprises assessing the degree of business risk based on the categorization of the information security characteristic according to a pre-defined risk level for the information security of the entity.

28. The method of claim 27, wherein assessing the business risk based on the categorization of the information security characteristic further comprises assessing the business risk based on the categorization of the information security characteristic according to a predefined level of readiness of the entity to deal with a risk to the information security of the entity selected from a group consisting of a complacent level of readiness, an acknowledgment level of readiness, an integration level of readiness, a common practice level of readiness, and a continuous improvement level of readiness.

29. The method of claim 28, wherein assessing the business risk further comprises assessing the business risk based on the categorization of the information security characteristic according to the complacent level of readiness indicative of a propensity of the entity to resignation to a current information security environment of the entity.

30. The method of claim 28, wherein assessing the business risk further comprises assessing the business risk based on the categorization of the information security characteristic according to the acknowledgment level of readiness indicative of a propensity of the entity to acknowledge a need to improve the information security of the entity.

31. The method of claim 28, wherein assessing the business risk further comprises assessing the business risk based on the categorization of the information security characteristic according to the integration level of readiness indicative of a propensity of the entity to integrate existing information security programs and services of the entity.

32. The method of claim 28, wherein assessing the business risk further comprises assessing the business risk based on the categorization of the information security characteristic according to the common practice level of readiness indicative of a propensity of the entity to customarily practice information security procedures for the entity.

33. The method of claim 28, wherein assessing the business risk further comprises assessing the business risk based on the categorization of the information security characteristic according to the continuous improvement level of readiness indicative of a propensity of the entity to continuously improve information security practices for the entity.

34. The method of claim 1, wherein assessing the business risk further comprises automatically assessing the business risk by a computer program.

35. The method of claim 1, further comprising selecting the entity for which to evaluate the information security.

36. The method of claim 35, wherein selecting the entity further comprises selecting the entity from one of a unit level entity, a business level entity, and an organization level entity.

37. The method of claim 1, further comprises assigning an evaluation team for the selected entity.

38. The method of claim 1, further comprising generating a recommendation for a security improvement related to the information security characteristic based at least in part on the assessed degree of business risk.

39. The method of claim 38, wherein generating the recommendation further comprises generating the recommendation for the security improvement based at least in part on the cost of the security improvement.

40. The method of claim 39, wherein generating the recommendation further comprises automatically generating the recommendation by a computer program.

41. A system for evaluating information security for an entity, comprising:

means for identifying at least one information security resource related to an information security area of the entity selected from a group of security areas consisting of an organizational environment area, a business commitment area, a policy and standards area, and an information security programs and services area of the entity;
means associated with the identifying means for receiving information about at least one information security characteristic for the identified information security resource;
means communicating with the receiving means for categorizing the information security characteristic according to a pre-defined hierarchy of information security risk levels associated with information security characteristics; and
means associated with the categorizing means for assessing a degree of business risk for the entity based on the categorization of the information security characteristic.

42. The system of claim 41, wherein the identifying means further comprises means for receiving a selection of the identified security information resource.

43. The system of claim 42, wherein in the means for receiving the selection further comprises a computer program.

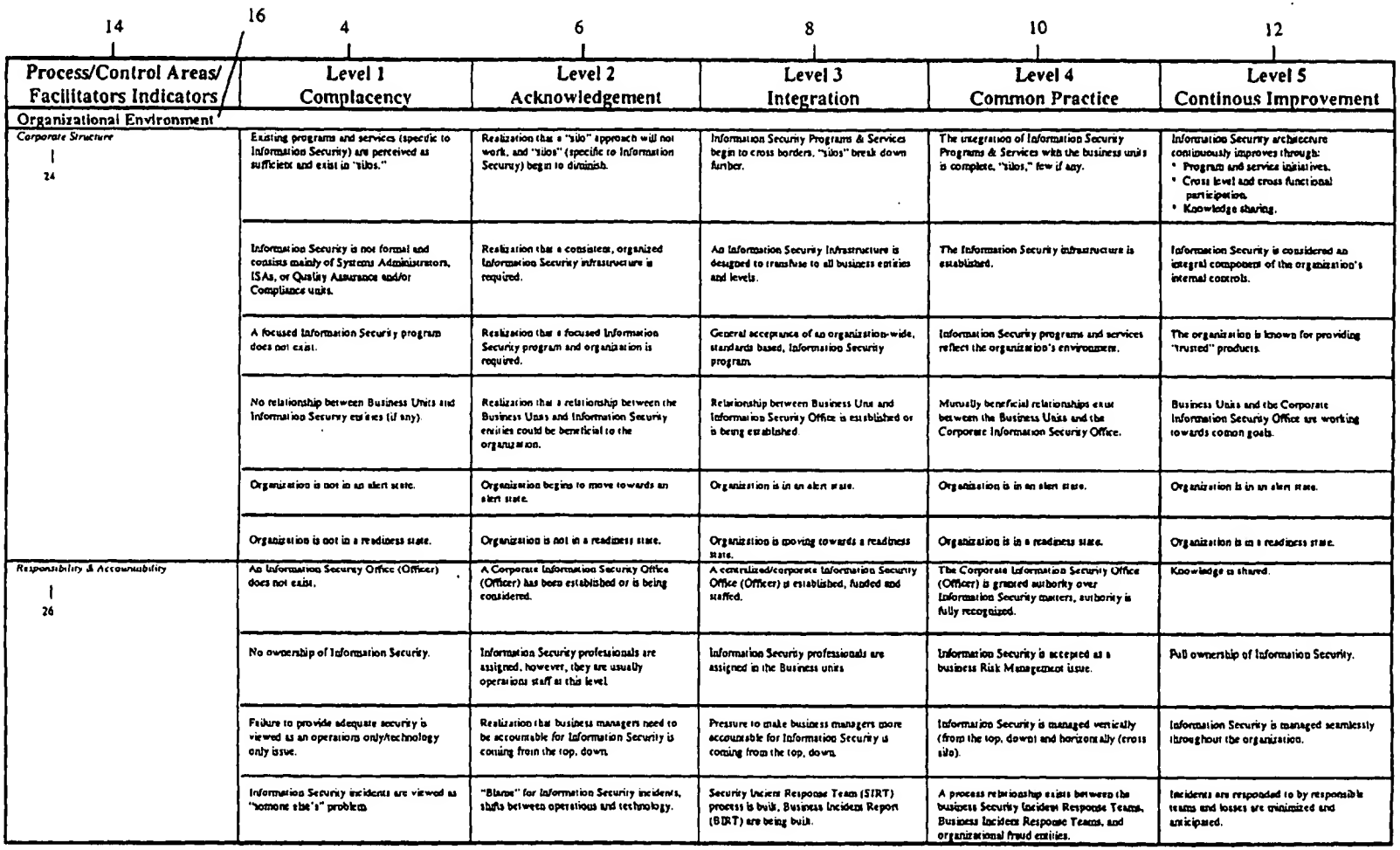
44. The system of claim 41, wherein the means for receiving the information further comprises a computer program.

45. The system of claim 41, wherein the means for categorizing the information security characteristic further comprises an information security evaluation model grid.

46. The system of claim 41, wherein the means for categorizing the information security characteristic further comprises a computer program.

47. The system of claim 41, wherein the means for assessing the degree of business risk further comprises an information security evaluation model grid.

48. The system of claim 41, wherein the means for assessing the degree of business risk further comprises a computer program.



Process/Control Areas/ Facilitators Indicators (14 / 16)	Level 1 Complacency (4)	Level 2 Acknowledgement (6)	Level 3 Integration (8)	Level 4 Common Practice (10)	Level 5 Continous Improvement (12)
Organizational Environment					
Corporate Structure (24)	Existing programs and services (specific to Information Security) are perceived as sufficient and exist in "silos."	Realization that a "silo" approach will not work, and "silos" (specific to Information Security) begin to diminish.	Information Security Programs & Services begin to cross borders, "silos" break down further.	The integration of Information Security Programs & Services with the business units is complete, "silos," few if any.	Information Security architecture continuously improves through: • Program and service initiatives. • Cross level and cross functional participation. • Knowledge sharing.
	Information Security is not formal and consists mainly of Systems Administrators, ISAs, or Quality Assurance and/or Compliance units.	Realization that a consistent, organized Information Security infrastructure is required.	An Information Security Infrastructure is designed to transfuse to all business entities and levels.	The Information Security infrastructure is established.	Information Security is considered an integral component of the organization's internal controls.
	A focused Information Security program does not exist.	Realization that a focused Information Security program and organization is required.	General acceptance of an organization-wide, standards based, Information Security program.	Information Security programs and services reflect the organization's environment.	The organization is known for providing "trusted" products.
	No relationship between Business Units and Information Security entities (if any).	Realization that a relationship between the Business Units and Information Security entities could be beneficial to the organization.	Relationship between Business Unit and Information Security Office is established or is being established.	Mutually beneficial relationships exist between the Business Units and the Corporate Information Security Office.	Business Units and the Corporate Information Security Office are working towards common goals.
	Organization is not in an alert state.	Organization begins to move towards an alert state.	Organization is in an alert state.	Organization is in an alert state.	Organization is in an alert state.
	Organization is not in a readiness state.	Organization is not in a readiness state.	Organization is moving towards a readiness state.	Organization is in a readiness state.	Organization is in a readiness state.
Responsibility & Accountability (26)	An Information Security Office (Officer) does not exist.	A Corporate Information Security Office (Officer) has been established or is being considered.	A centralized/corporate Information Security Office (Officer) is established, funded and staffed.	The Corporate Information Security Office (Officer) is granted authority over Information Security matters, authority is fully recognized.	Knowledge is shared.
	No ownership of Information Security.	Information Security professionals are assigned, however, they are usually operations staff at this level.	Information Security professionals are assigned in the Business units.	Information Security is accepted as a business Risk Management issue.	Full ownership of Information Security.
	Failure to provide adequate security is viewed as an operations only/technology only issue.	Realization that business managers need to be accountable for Information Security is coming from the top, down.	Pressure to make business managers more accountable for Information Security is coming from the top, down.	Information Security is managed vertically (from the top, down) and horizontally (cross silo).	Information Security is managed seamlessly throughout the organization.
	Information Security incidents are viewed as "someone else's" problem.	"Blame" for Information Security incidents, shifts between operations and technology.	Security Incident Response Team (SIRT) process is built, Business Incident Report (BIRT) are being built.	A process relationship exists between the business Security Incident Response Teams, Business Incident Response Teams, and organizational fraud entities.	Incidents are responded to by responsible teams and losses are minimized and anticipated.

2

FIG. 1

EP 0 999 489 A2

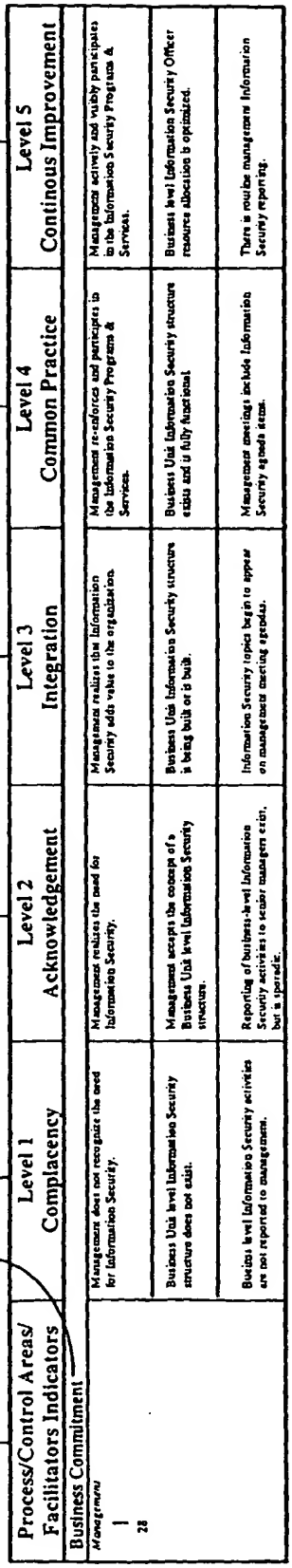

14
18
4
6
8
10
12
Process/Control Areas/ Facilitators Indicators
Level 1 Complacency
Level 2 Acknowledgement
Level 3 Integration
Level 4 Common Practice
Level 5 Continous Improvement
Business Commitment
Management
1
28
Management does not recognize the need for Information Security.
Management realizes the need for Information Security.
Management realizes that Information Security adds value to the organization.
Management re-enforces and participates in the Information Security Programs & Services.
Management actively and visibly participates in the Information Security Programs & Services.
Business Unit level Information Security structure does not exist.
Management accepts the concept of a Business Unit level Information Security structure.
Business Unit Information Security structure is being built or is built.
Business Unit Information Security structure exists and is fully functional
Business level Information Security Officer resource allocation is optimized.
Business level Information Security activities are not reported to management.
Reporting of business-level Information Security activities to senior managers exist, but is sporadic.
Information Security topics begin to appear on management meeting agendas.
Management meetings include Information Security agenda items.
There is routine management Information Security reporting.
2

FIG. 2

14 4 6 8 10 12

Process/Control Areas/ Facilitators Indicators	Level 1 Complacency	Level 2 Acknowledgement	Level 3 Integration	Level 4 Common Practice	Level 5 Continous Improvement
Business Commitment - Cont'd.					
Funding 30	Information Security budgets are small or non-existent.	Budgeted dollars are spent on high-priced security technologies, usually data center centric.	Budgeted dollars begin to include funding for Information Security Programs and Services.	Budgeted dollars are routinely allocated to Information Security Programs and Services and infrastructure.	Information Security Programs and Services are planned, budgeted and routine (security economics)
	Management funds only critical or mandated Information Security activities.	Management willingly allocates funds for Information Security products and systems, which are usually operations-oriented at this level.	Management willingly allocates funds for all information Security products and systems.	Management willingly allocates funds based on known return on investments.	Recovery costs are well understood.
Incident Management (BIRT) (Business Incident Response Teams) 32	Information Security incidents are managed as crisis events.	Based on lessons learned some response teams are being built within the business units.	Business Incident Response Team (BIRT) are being built.	Business Incident Response Teams (BIRTs) are built and fully functional, incidents are responded to with corrective actions.	Business Incident Response Teams (BIRTs) evolve with the environment.
Incident Management (SIRT) (Security Incident Response Team)	Information Security incidents are managed by crisis management teams.	Organization realizes need for SIRT and begins to build.	SIRT process is established and functioning.	SIRT process is coordinated with BIRT processes.	Threats are continually re-evaluated based on changing threat population and security incidents.
Awareness & Education 34	No sense of awareness.	Recognize the need for Information Security awareness programs and education.	Awareness and educations programs are being built.	The practice of information security is considered "daily."	Information Security awareness and education is continuous through: • Program and Service initiatives. • Cross level and cross functional participation. • Knowledge sharing.
	Awareness programs and/or educational materials are minimal or not available.	Levels of awareness vary throughout the organization.	Overall awareness becomes heightened based on programs, e.g., all new hire packages include Information Security training materials.	Information Security is a common business practice, where Information Security training is used to augment awareness.	The practice of Information Security is considered a component of the corporate culture (second nature).
	Threats are not known and/or well understood.	Some threats are known, but are not widely understod or analyzed.	Threats are known and understood by most of the business units.	Threats are known reported and analyzed.	Threat management is practiced.
Operations 36	Configuration change controls are not formal or centralized.	Change management and configuration management controls are defined but are not coordinated.	Change management and configuration management controls are coordinated.	Change management and configuration management controls are consistent.	Implementation cycles are rapid.
	Minimal safeguards are mandated (data center/network centric).	Critical Information Security safeguards are mandated to rpotect corporate assets.	Businesses build Information Security safeguards which are mutually beneficial.	Mutually beneficial process relationships exist between the business units.	Information Security technical research activities are encouraged to be consistent with rapidly changing environments.
Information Ownership 38	Information owners do not exist - responsibility/authorizations is lacking.	Realization that there is a need for information ownership and that accountability for information assets should be assigned to the "right people."	Accountability for information assets may be assigned to the "right person," some senior-level information owners (with responsibility) have been identified.	Information assets have been assigned owners (with authority) at the business/customer/user level.	Information ownership is realized.
	Information assets are not considered as separate entities requiring security.	Realization that information assets have value and need to be protected.	The level of protection required for information assets is considered when making decisions.	Determining the level of protection required for information assets is routine.	The organization fully values their information assets.
Information Classification (Risk) 40	Information is not classified, no relationship to business risk.	Realization that information must be "classified" as a function of risk to the business unit.	Businesses information classification may or may not be based on risk.	Information Security classifications are considered a coimponent of the Business Risk analysis process.	Information classification is continually reviewed for optimal risk/security benefits.

2

FIG. 3

EP 0 999 489 A2

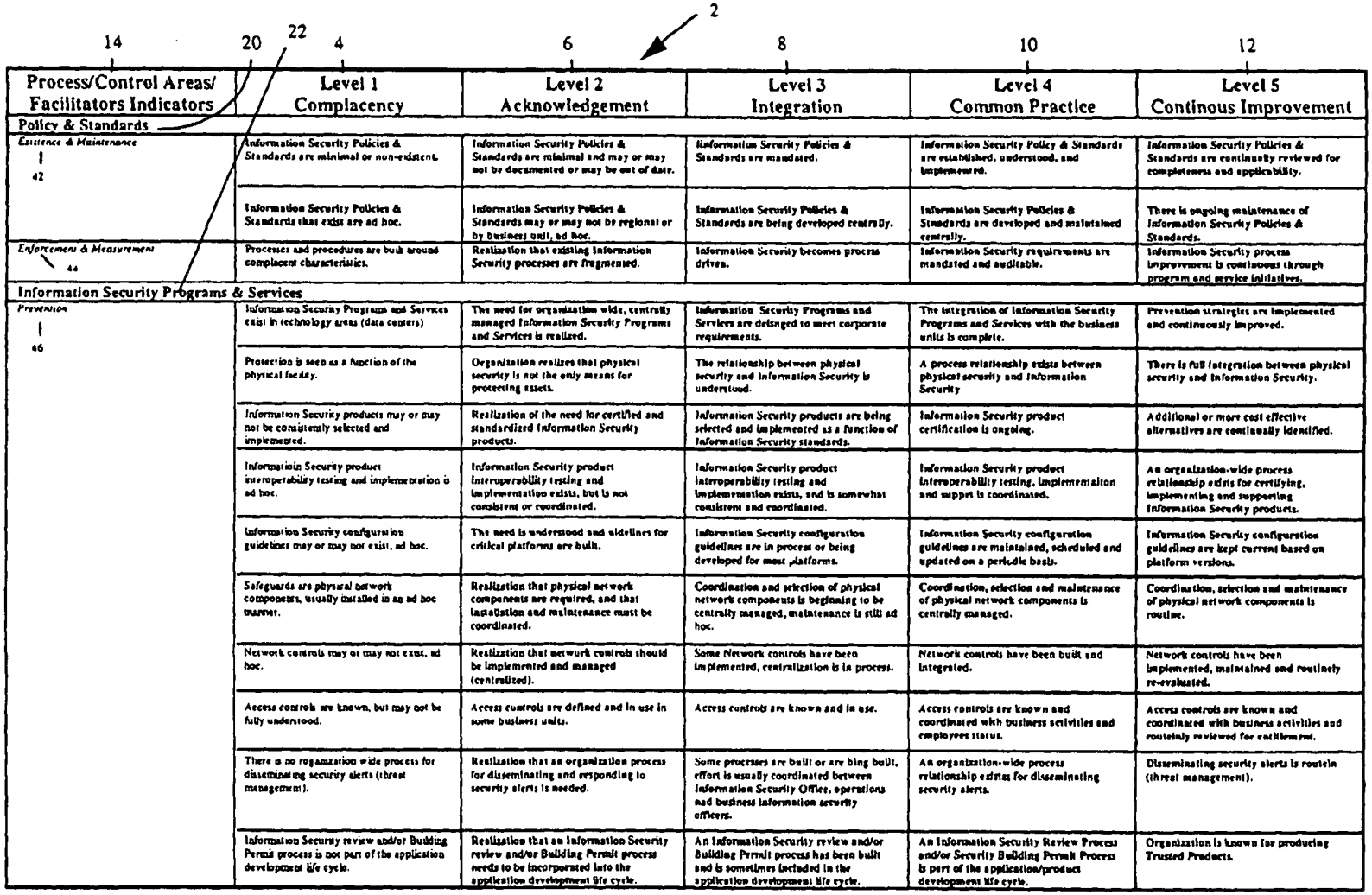


FIG. 4

EP 0 999 489 A2

14 4 24 6 8 10 12

Process/Control Areas/ Facilitators Indicators	Level 1 Complacency	Level 2 Acknowledgement	Level 3 Integration	Level 4 Common Practice	Level 5 Continous Improvement
Information Security Programs & Services - Cont'd.					
Detection 48	Network audit controls °e.g., logging) are built around complacent characteristics.	Realization that network audit controls should reflect Information Security Policies & Standards, and risk/impact to network availability.	network audit controls, based on Information Security Policies & Standards are being built into network (data center) operating procedures.	network audit controls, based on Information Security Policies & Standards are built into network operating procedures.	Network audit controls, based on Information Security Policies & Standards are used routinely.
	Risk Review/Internal Audit programs are built around complacent characteristics.	Realization that Risk Review/Internal Audit programs should reflect Information Security Policies & Standards and risk/impact to the business unit.	Risk Review/Internal Audit programs begin to reflect Information Security Policies & Standards and risk/impact to the business unit.	Risk Review/Internal Audit programs continue to evolve with Information Security Policies & Standards and risk/impact to the business unit.	A process relationship between Risk Review/Internal Audit programs and Information Security Policies & Standards and the business units.
	Help Desks are used to report information security incidents, no escalation.	Incidents are still reported through a Help Desk, however, escalations have been refocused.	Help Desks is used to report incidents, some escalation to BIRT/SIRT may exist.	Help Desk is used to report incidents, escalation to BIRT/SIRT process is fully implemented.	Help Desk is used to report incidents, escalation to BIRT/SIRT process is routine.
	There is no formalized Corporate/organizational incident reporting or tracking.	An informal corporate/organizational incident reporting and tracking process may exist.	An organization-wide process relationship is being developed/implemented for reporting Information Security incidents.	An organization-wide process relationship exists for reporting Information Security incidents.	Organization-wide reporting of Information Security incidents are routine.
	Viruses are handled as isolated incidents.	Realization that viruses are not specific hardware or software incidents and that they require immediate remedy.	Virus reporting is centralized.	Virus incidents are tracked and reported.	Virus incident trending, tracking and reporting is available.
	Ethical Hacking (Infrastructure/Internet) procedures do not exist - no intrusion detection.	Realization that Ethical Hacking (Infrastructure/Internet) procedures are necessary - intrusion detection.	Ethical Hacking (Infrastructure/Internet) procedures have been initiated - intrusion detection.	Ethical Hacking (Infrastructure/Internet) procedures are mandated required - intrusion detection.	Ethical Hacking (Infrastructure/Internet) procedures are routine - intrusion detection becomes a source of threat management.
Verification 50	Information Security incidents are not reported and tracked as such.	Realization that tracking Information Security incidents adds value as an incident management tool.	Information Security incidents may or may not be tracked and reported as such.	Information Security incidents are tracked and reported as such.	Information Security incidents are tracked and reported on a routine basis.
	Information Security Metrics are not collected or considered.	Management realizes the need for the collection of Information Security based metrics.	Information Security Metrics are collected consistently or with some consistently.	Information Security Metrics are collected, analyzed, and used to make decisions.	Information Security metrics are used for decision making, trending, and threat management.
	Business Unit self-assessments do not include Information Security vulnerability assessments.	Realization that a Information Security vulnerability is a viable component of the business unit self-assessment process.	Information Security vulnerability assessments are performed, may or may not be a component of the self-assessment process.	Information Security vulnerability assessments have been incorporated into the self-assessment process.	Information Security vulnerability assessments are routine (threat management/threat aversion).

FIG. 5

EP 0 999 489 A2

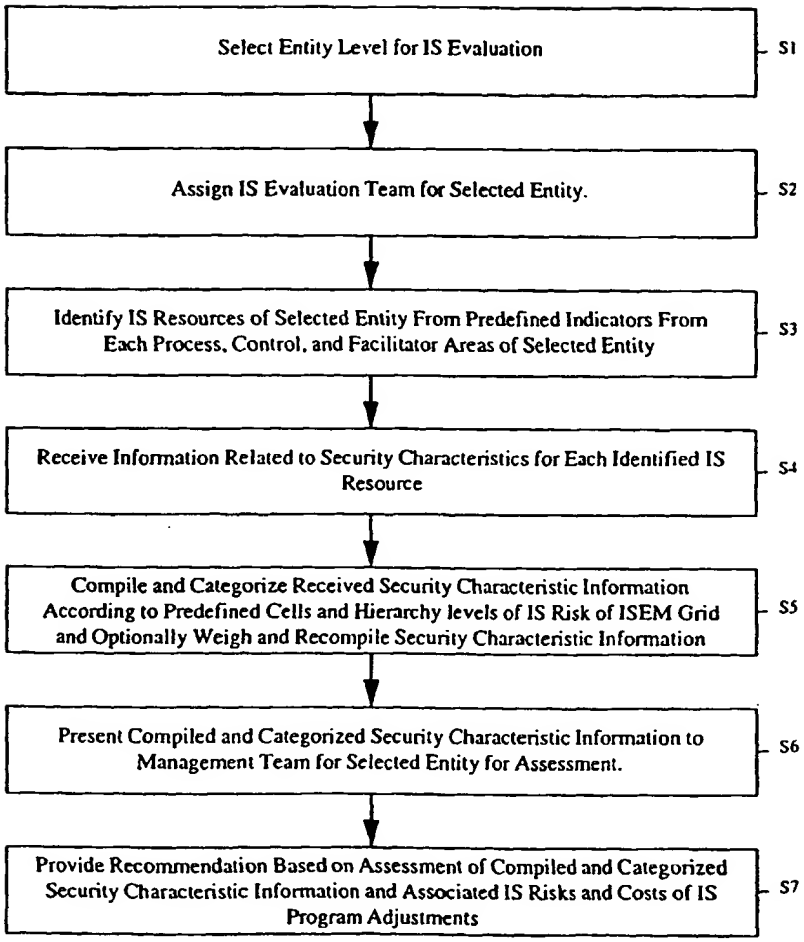

Select Entity Level for IS Evaluation
S1
Assign IS Evaluation Team for Selected Entity.
S2
Identify IS Resources of Selected Entity From Predefined Indicators From Each Process, Control, and Facilitator Areas of Selected Entity
S3
Receive Information Related to Security Characteristics for Each Identified IS Resource
S4
Compile and Categorize Received Security Characteristic Information According to Predefined Cells and Hierarchy levels of IS Risk of ISEM Grid and Optionally Weigh and Recompile Security Characteristic Information
S5
Present Compiled and Categorized Security Characteristic Information to Management Team for Selected Entity for Assessment.
S6
Provide Recommendation Based on Assessment of Compiled and Categorized Security Characteristic Information and Associated IS Risks and Costs of IS Program Adjustments
S7

FIG. 6

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 11/30 — A1

(11) International Publication Number: WO 00/70463

(43) International Publication Date: 23 November 2000 (23.11.00)

(21) International Application Number: PCT/US00/12724

(22) International Filing Date: 9 May 2000 (09.05.00)

(30) Priority Data:

60/134,090	14 May 1999 (14.05.99)	US
60/144,319	16 July 1999 (16.07.99)	US
09/506,024	17 February 2000 (17.02.00)	US

(71) Applicant: L-3 COMMUNICATIONS CORPORATION [US/US]; 600 Third Avenue, 34th Floor, New York, NY 10016 (US).

(72) Inventors: BUSH, Stephen, F.; 9 Sable Terrace, Latham, NY 12110 (US). BARNETT, Bruce, G.; 64 Calhoun Drive, Troy, NY 12182 (US). GALUP, Luis, E.; 153 Oak Brook Commons, Clifton Park, NY 12065 (US).

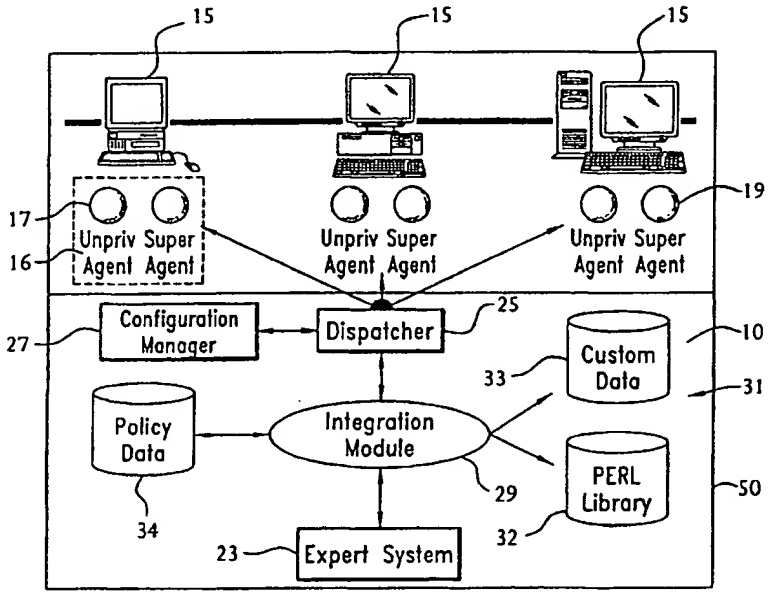
(74) Agents: ROCCI, Steven, J. et al.; Woodcock Washburn Kurtz Mackiewicz & Norris LLP, One Liberty Place – 46th Floor, Philadelphia, PA 19103 (US).

(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.

(54) Title: APPARATUS AND METHODS FOR ANALYZING MULTIPLE NETWORK SECURITY VULNERABILITIES



(57) Abstract

A method and apparatus for analyzing multiple computer network vulnerabilities, capable of gathering vulnerability data from one or more hosts (15) within the network and generating a directed graph from the gathered vulnerability data. Nodes in the graph represent vulnerabilities within the network. Paths between nodes are edges, and represent probability values associated with moving from one vulnerability to another.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

APPARATUS AND METHODS FOR ANALYZING MULTIPLE NETWORK SECURITY VULNERABILITIES

TECHNICAL FIELD

This invention relates generally to computer data networks and, specifically, to a network vulnerability analysis tool.

BACKGROUND OF THE INVENTION

As the world transitions to more standardized digital communications driven by the various international standards organizations, and as interoperability becomes the norm for both communication networks and processing systems, information systems have and will become the targets for penetration, deception, and/or destruction by adversaries. Absent a constant vigilance and administration, any secure system will become more vulnerable over time. This is due to both internal and external sources. Internally, as access privileges are granted to new users or increased to existing users (including unauthorized access), the security profile of the system changes, usually for the worse. Client/server architectures, remote access, and trusted networks exacerbate the problem.

Externally, as the profile of the network becomes more familiar to an intruder and as penetration methods become more sophisticated, the system becomes less secure.

In the beginning of computer security, when there was little or no network connectivity, most of the attention was drawn towards insider threats and internal computer misuse. For instance, a user is granted a particular set of privileges and abuses it by accessing unauthorized files or modifying data for his or her own purpose.

During the 1980s and 1990s, as the Internet grew at an astronomical rate - from under 2,000 hosts in October 1985 to currently over 18 million hosts - firewalls drew a lot of attention. Firewalls allow companies and other entities to have partial connection to the Internet, while retaining some amount of physical isolation. Corporations were quick to create gateways from their internal networks to the Internet and used firewalls to protect their security.

Now, it appears that the focus is once again on internal threats. Many corporate intranets are now larger than the entire Internet was in the mid-1980s. With trusted hosts providing connectivity between different business units and corporate partners, companies now have a number of machines that are effectively behind the corporate firewall. Managing the complexities of connectivity between all of these hosts forces system administrators to view firewalls as only a complement to other security measures.

A system administrator has a number of powerful security and audit tools available to deal with the aforementioned problems. Many of these tools are freely available. Two major classes of system security tools that address the issue of internal threats and system integrity are 1) vulnerability assessment systems, and 2) intrusion detection systems. The former is proactive; it looks for potential system vulnerabilities. The latter is reactive; it attempts to detect that an attack or intrusion has occurred.

The present invention relates to a vulnerability assessment system, of which two types are now known to exist:

1) Single system, internal privileged assessment using software packages running on a single system with superuser privileges. One example of such a system is Computer Oracle and Password System (COPS), a UNIX security status checker which can be retrieved via anonymous File Transfer Protocol (FTP) from cert.org in -/pub/tools/cops; and 2) Distributed, external, non-privileged assessment packages that can scan several systems for weaknesses. An example of such a package is the Security Administrator Tool for Analyzing Networks (SATAN). SATAN recognizes several common networking-related security problems, and reports the problems without actually exploiting them.

In general, these packages are difficult to use, and hard to maintain. Because databases may not be updated as new information is acquired, it is difficult to keep the checks up-to-date. A person must walk from system to system with a floppy disk to check the security of each system. Even so, it is difficult to know if all of the checks are being performed properly. This is because checks are often hidden deep inside scripts that do not have any obvious relationship to the files being exercised. To learn what list of checks is being performed requires examining the source code in detail. Such an examination is burdensome and time consuming.

Another problem is the lack of a clear security policy. System Administrators typically leave the checking programs alone, or else run all of the tests, and then remove the tests that cause problems. There is no clear definition of policy for the system, and no clear relationship between the policy, the tests performed, and the tests ignored. Therefore, it is difficult to know if a system is vulnerable, and how a particular feature relates to the vulnerability.

A third flaw in the architecture of these systems is the lack of a clear hierarchy of features in each system. Currently, code is written for a single platform, and when other platforms are added, the code is modified with branch conditions for each architecture. This makes the code hard to follow, and makes it hard to know what check is being

performed.

Standard vulnerability assessment techniques are suitable for finding major security problems and may help protect a system from a brute force attack. However, they offer no defense against a hacker using a series of techniques to gain access to a system through a series of weaknesses. It is possible for a hacker to use a series of techniques to gain access to a system through a series of weaknesses of least privilege.

What is needed, then, is a vulnerability assessment tool that can diagnose and analyze multiple security vulnerabilities of a computer data network and the manner in which security safeguards strengthen those weaknesses, and can provide an easily understood display (both in 2- and 3-dimensions) of the network and its vulnerabilities.

SUMMARY OF THE INVENTION

The present invention broadly comprises apparatus and methods for analyzing multiple computer network vulnerabilities, comprising gathering vulnerability data from one or more hosts within the network; and, generating a directed graph from the gathered vulnerability data where nodes in the directed graph represent vulnerabilities within the network. Paths between nodes are defined as edges, and the edges represent probability values associated with moving from one vulnerability to another. The invention also includes two separate methods of analysis: a probabilistic approach and a maximum flow approach, both accomplished by computer software implementation of algorithms. The invention displays the results of the analysis in a number of ways, and is capable of displaying a topological display of the computer network vulnerabilities.

These and other objects, features and advantages of the invention will become readily apparent to those having ordinary skill in the art upon a reading of the detailed description of preferred embodiments and the appended claims

in view of the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a representative software architecture that can be used in association with the present invention.

Figure 2 is a representative common Application Program Interface (API) and integration module that can be used in association with the present invention.

Figure 3 illustrates a Central Assessment System (CAS) and agent dialogue in a representative secure communications protocol that can be used in association with the present invention.

Figure 4 illustrates a representative secure communications protocol that can be used in association with the present invention.

Figure 5 is a network vulnerability assessment graph.

Figure 6 is an example vulnerability graph illustrating about 2,000 vulnerabilities found on a few nodes of a network thought to be reasonably secure.

Figure 7 is an example vulnerability graph generated by the invention.

Figure 8 is a maximum flow result graph of a network.

Figure 9 illustrates data grouped by attack paths.

Figure 10 illustrates more detailed data about attack vectors.

Figure 11 quantifies the attack paths shown in Figure 4.

Figure 12 is an example of security safeguard allocation.

Figure 13 graphs the effect on vulnerability of security safe-guard allocation.

Figure 14 is an example of an attack in progress.

Figure 15 graphs the probability of monitoring an attack during its occurrence.

Figure 16 is a three-dimensional display showing the

probability of monitoring an attack during its occurrence given multiple independent detection systems.

Figure 17 shows the startup button of the software program of the invention.

Figure 18 illustrates the start-up screen of the software program of the invention.

Figure 19 illustrates the GML Open Window.

Figure 20 illustrates an example vulnerability chain.

Figure 21 illustrates a vulnerability analysis probabilistic result for the chain illustrated in Figure 19.

Figure 22 illustrates a screen capture of a vulnerability analysis graph result.

Figure 23 illustrates a vulnerability analysis maximum flow result.

Figure 24 illustrates a vulnerability analysis graph maximum flow result.

Figure 25 is an illustration of articulation points of the graph shown in Figure 24.

Figure 26 is an alternative tree down depiction of the graph node positions, showing the attacker as the root.

Figure 27 illustrates a vulnerability graph before nodes have been grouped.

Figure 28 is a screen capture similar to that shown in Figure 27, but taken after the nodes have been grouped.

Figure 29 illustrates the group control window of the invention.

Figure 30 illustrates how to add a new node to a vulnerability graph to facilitate analysis of a "what if" scenario.

Figure 31 is a screen capture of a window used to change a node label.

Figure 32 is a screen capture of a window used to modify an edge.

Figure 33 is a screen capture of the resulting graph after a node and edge have been added.

Figure 34 illustrates the textual result of a

probabilistic analysis run on the modified graph of Figure 33.

Figure 35 illustrates the graphical result of a probabilistic analysis run on the modified graph of Figure 33.

Figure 36 is a representative topological map of vulnerabilities in a network created by the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

A system 100 for analyzing multiple computer network vulnerabilities in a computer network comprising a security computer and a plurality of host computers 15 is illustrated in Figure 1. According to the embodiment shown in Figure 1, a Central Assessment System (CAS) 10 resides on security computer 50. CAS 10 is in communication with a plurality of software agent sets 16. Each software agent set 16 resides on a respective host computer 15.

Each software agent set 15 includes an unprivileged agent 17 and a super agent 19. Unprivileged agent 17 is configured to communicate with CAS 10 via BSD socket connections. Super agent 19 is configured as a proxy server and as such, is accorded root privileges and network access permissions which unprivileged agent 17 does not have, in accordance with known techniques for configuring proxy servers. Typical authentication and encryption techniques are applied to communications between CAS 10 and unprivileged agent 17 and between unprivileged agent 17 and super agent 19 to prevent unauthorized access to privileged information accessible by super agent 19.

According to one embodiment of the invention, security computer 50 is adapted with a UNIX operating system and is ideally positioned in a highly secure location, such as a locked room having restricted access. The architecture of computer 50 is an automated Unix system management system, which monitors hosts connected by a network and reports proactively on system degradation and vulnerable configurations. CAS 10 resides on computer 50 and includes an

Expert System (ES) 23, a Dispatcher 25, a Configuration Manager (CM) 27, an Integration Module (IM) 29, and one or more supporting databases 31. Supporting databases 31 include PERL library 32, custom data 33 and policy data 34. Both CAS 10 and software agent set are implemented in the JAVA programming language. It should be appreciated that, although the present invention is implemented in the JAVA language in a preferred embodiment, the claims of the invention are not so limited, in that the invention could be readily implemented in other languages by one having ordinary skill in the art.

ES 23 comprises a plurality of reasoning modules which implement rules upon which diagnoses are based. In addition, ES 23 contains status and configuration data about networked UNIX nodes in order to diagnose vulnerable systems. The software agents 16 provide data about different hosts 15 and accounts. The ES 23 may ask the agents 16 for information about each host 15 or account. The Perl Library 22 contains a collection of methods that can be dynamically downloaded to the software agent. This allows the rules in the ES 23 to be reused, as it may have rules and understand the class or type of object, as well as the methods used to obtain information from the objects. It can know how some values returned from these queries indicate particular symptoms of system problems. Based on this information, the ES 23 may decide to query more information, initiate a vulnerability in the database, or take corrective action.

The Dispatcher 25 functions as a message switchboard between the ES 23 and software agents 16. The CM 22 provides basic configuration information about the network and hosts 15. The Custom Database 33 contains class instances of the network (users, hosts, directories, and vulnerabilities). The Policy database 34 is discussed *infra*.

The IM 29 is the mechanism by which the ES 23 and the software agents 16 access system and network information. It also is the interface for the system to other security applications. The outputs of various security tools are instantiated into common objects via the IM 29.

The software architecture described above was developed based on the premise that the degree of protection from information warfare attacks is highly dependent on the amount of time and effort invested in building and maintaining system security defenses. The solution offered by the present invention is to off load the work and tasks of network management to software agents. Each agent 16 operates independently, but they all cooperate in monitoring the system. Collectively, the software agents 16 achieve the overall goal of system monitoring and intrusion detection. This approach provides significant advantages in terms of scalability, flexibility, and efficiency.

The software agents 16 are TCP-based server programs started up by the root user. Written entirely in Perl 5 and less than 50KB in size, the software agents 16 are designed to have minimal effect on host performance. The agent code does not reside on any network disk. This prevents an intruder from modifying the agent code to affect agent behavior.

The software agents 16 are dynamically extensible because methods and instructions can be downloaded to them from the CAS 10. Because the software agents 16 do not contain a collection of security checks and information-gathering modules embedded in them, this greatly helps reduce the amount of space the agents occupy in memory. The agent's actions are not scripted; the CAS 10 can dynamically choose which actions to invoke, and in what sequence, in response to the state of its external environment.

The CAS 10 communicates to the unprivileged agent 17 by sending it a method and the reference to an object to which the method is to be applied. The object is referenced by the object type, followed by the name of that object. For example, to reference the route account on machine tango, the object reference would be account/tango/root. Basic uploadable methods include:

scan_all_patches - given a reference to a host object, an agent will scan for the correct installation of security patches for a particular operating system. This is

accomplished by taking the MD5 signature of every file associated with a particular patch and comparing it to the signature of the file currently on the system. Operating systems that are currently supported include SunOS 4.1.3, Sun OS 4.1.3 Ul, Solaris 5.2, Solaris 5.3, Solaris 5.4, and Solaris 5.5.1. The patch information is updated regularly by the CAS via ftp.uu.net (the official distribution for SUN security patches).

scan_trojan_directories - given a reference to particular directory or user search path, the agent will scan for trojan horse vulnerability. This is accomplished by recursing through every file and directory to determine which files are group or word writable. The method can also handle soft and hard links.

read_all_data - this is a generic method that allows an agent to read instantiated vulnerabilities from the custom database. This will basically allow different security applications to communicate to the agents. The Integration Module takes the input for any arbitrary number of security applications and instantiates vulnerabilities into the common OO database as shown in Figure 2.

An IDS can generate vectors and the IM can instantiate vulnerabilities into the common OO database. A security agent reads the database to gather security information. Other information reporting methods include:

report_all_vulnerabilities -list all vulnerabilities on a particular machine

dump_root_vulnerabilities - list all root vulnerabilities on a particular machine

object_count - the number of objects the agents knows about from the custom database

The count of the number of vulnerability instances is a primitive measure for system administrators to show progress in securing their networks. The present invention as described *infra* provides a closer examination of each vulnerability listed to clearly indicate what steps are

necessary to reduce the number of instantiated vulnerability objects.

The interface between the privileged agent and non-privileged agent must be secure. An intruder who has access to the interface cannot ask the system to weaken the system security. The interface is designed to be as simple as possible, as complex systems are harder to secure.

Consider an example where the CAS asks the unprivileged agent on a host to gather some information. The unprivileged agent wants to examine the security of a file, and does not have permission to do so. It asks the privileged agent to get the information, and pass the results back to the non-privileged agent. This dialogue is shown in Figure 3.

The format of each request is a packet containing the following four fields: type, length, data, and signature. The type field identifies the type of packet, the type of signatures used, and the format of the packet. Some packets could contain binary information, others ASCII. The length indicates the amount of data (and/or the length of the signature field). The data is the command issued. It is always encrypted using DES-ECB. The signature can vary with packet type (some types may not have a signature field). One of the common signatures will be the MD5 hash of the data, encrypted using the secret key shared between the two systems. In this manner, the integrity of the command, and authentication, can be confirmed before the command is executed.

For each communication session between either the CAS and the unprivileged agent or between the unprivileged agent and the super agent, there are authentication mechanisms and an exchange of keys. This security protocol is shown in Figure 4.

There is a secret master key and secret master TCP port that the two entities use to establish a secure communications channel. The shared key and port is known only between the entity pair. The master key and a master TCP port are used to establish a session key and session port. At each intermediate step, a random challenge is issued to

authenticate the sender and to prevent message replay. Once the secure communication channel is established, the two entities can continue to communicate, and no additional handshaking is necessary. Table 1 below shows the contents of the payload, the encryption key used, and the TCP port used at each step of the protocol.

Table 1. Payload, Key, and Port for Protocol

Stage	Payload	Encryption Key	TCP Port
1	Request for Conversation	Master	Master
2	Random Challenge	Master	Master
3	Random Challenge and Session Key	Master	Master
4	Random Challenge and Session Port	Session	Master
5	Random Challenge and Information Request	Session	Session
6	Random Challenge and Information	Session	Session

The privileged agent has a database and caching

mechanism that identifies the list of commands, and the security requirements necessary for each command. For instance, any system might be able to see if the privileged agent is running, and obtain the revision of the agent. Or the agent may refuse to acknowledge an outside query. The choice is up to the agent, and the person who installed the agent.

It is unlikely that a complete list of security problems exists. New ones are always being reported. The architecture is not intended to be a list of unrelated problems, but an organization based on operating system, release level, and policies. The goal is to have an integrated knowledge base, so that an intelligent system can react to exploitation problems without disabling the entire network. The Security Policy Database (SPD) provides a structured, quantifiable way to record information about systems and their flaws as they are discovered.

There is a direct relationship between the object classes and the information in the database. This object model allows evolution and code reusability, allowing modification of classes with minimum impact. Five kinds of items in the SPD are as follows:

Objects: Objects are resources and actors on a computer system. They may be such concrete or abstract things as files, peripherals, network ports, and users. Objects are represented by a list of labeled data values.

Systems: Systems are the active software systems providing services on a network. Examples of systems are the kernel, mail and Web servers, and the file system.

Abilities: Abilities are the actual services available from systems that act upon or at the request of objects. Abilities are represented by a set of preconditions indicating states of objects necessary to use the ability, and a set of post-conditions indicating changes to the objects from the use of the ability. Abilities may be intentional, such as the ability for the owner of a file to modify it. They may also be unintentional, such as the ability of network user to gain root access from certain versions of the mail system.

Policy: Policy describes what is allowed and disallowed (*e.g.*, world readable files, no passwords in the clear over the wire, authenticating based on IP address, File Sharing, unauthenticated mail, set-uid files on home directories, finger, "." in a search path, *etc.*). The policy has impact levels. That is, each policy should indicate the importance of the policy. A simple rating system may include states: (Allow, Should, Should Not, Disallowed, Unknown). A policy may start out as "Unknown/Don't Care", then change to "Should Not", and later change to "Disallowed" - based on conditions. Other schemes may also be appropriate. One option is to have a variable policy, with a range of values, ensuring genetic variability in systems.

Regions: Regions represent the organization of processes, corresponding to a chain of command. A relationship between bosses and workers is defined by this object class, and its relation to other objects of the same class. One model may be simple: Each region has one boss, and each regional boss may have several sub regions reporting to it. Other models may include two levels of command for each region, or shared authority. Regions group systems, and may be geographical, or authoritative.

Figure 5 is an instance of a typical security object model. Just as a virus uses host cells to reproduce, an attacker enters the network and can choose from a variety of vulnerabilities to take control of the network. In Figure 5, an attacker decrypts the password of User 2 on Host 1. The cost to the attacker is (10,0,0,0) which is a vector of the form: (password decryption, NFS spoofing, host spoofing, application fault). From that point, an attacker may illegally modify File System 1 on Host 1 with a cost of (0, 10, 0, 5), or decrypt the password for User 1 on Host 1 with a cost of (10, 0, 0, 0). Host 3 in Figure 5 is an example of host spoofing in which the attacker can use File System 1 on Host 1 in order to change the identity of a host. From the graph shown in Figure 5, it should be understood that the network

is as vulnerable as the weakest path.

The preceding description is intended to set the background, by way of example, for a representative object model, software architecture, software agents and secure communications protocol that may be used in conjunction with the present invention. It should be understood, however, that other models, architectures, types of software agents and communication protocols may be used, and thus the preceding description is not necessary to enable one having ordinary skill in the art to make and use the invention, which is described here below.

In the description that follows, the method and apparatus of the invention will be referred to as the "tool" for convenience. The tool is a Java-based network vulnerability and analysis tool.

Figure 6 displays 2000 vulnerabilities found on a few nodes of a network that were thought to be reasonably secure. Vulnerabilities are displayed in Figure 6 by host and type. The number along each edge of the graph represents the number of opportunities available to the attacker to reach the next vulnerability. Using this information, the tool has several algorithms for determining the vulnerability, V.

In a preferred embodiment, the tool uses two fundamental techniques for determining vulnerability to attack. Both techniques are based on determining "insecurity flow." The tool can display the results at various levels of detail, including the individual host level, vulnerability types, host types, or individual vulnerabilities.

The tool can automatically generate a directed graph representing the security vulnerabilities of a network. This information is gathered from the network security software agents described above. The security vulnerability graph for a typical network can be extremely dense; however, the object-oriented nature of the security model described above is useful in choosing the level of abstraction required. For example, it may be possible to display the vulnerability graph for Unix hosts in general and hide the details of individual

Unix variants. The tool determines the degree to which specified targets within the network can be compromised. The vulnerability chain is displayed as a directed graph. Nodes represent vulnerabilities whose security may be compromised and edges represent paths from one vulnerability to another. The larger the value of the edge label, the greater the vulnerability. Figure 7 shows an example vulnerability graph generated by the tool.

One of the security assessment operations the tool can perform is to determine the vulnerability of a particular entity given an attack on a particular node. The target entity Host C Vulnerability 4 is identified by a white cross-hair in Figure 8 and the attacking node is labeled Attacker with the flow identified by the label of its connecting path. The optimal vulnerability path is the sum of flows into node Host C Vulnerability 4 as shown in Figure 8, a flow strength of 6.0.

In Figure 8, the optimal path that the attacker can take to reach the target is shown. Thus the tool provides the ability to examine how the placement of security safeguards such as intrusion detectors within the network affect total network security. In effect, this tool becomes a security modeling tool, where one can experiment with the placement of security safeguards representing such entities as firewalls, intrusion detectors, and access lists. These can be positioned at various locations in order to determine network security.

The tool allows various types of node groupings in order to help visualize the vulnerability paths. In Figure 9, all object types are grouped together. The nodes could also be grouped by such characteristics as hostname or subnetwork. In Figure 10, the vulnerabilities which have been identified and grouped as vectors to vulnerability targets have been expanded to show more detail about the individual vulnerabilities. In Figure 11, all 40 parent objects of sun4/bin are grouped within a single node. Also note that the root account is clearly visible as reachable through the vulnerability path.

It becomes clear that defensive security safeguards cannot be studied independently of offensive information warfare. Thus, a tool that can accurately study both is desirable. Initially, perfect information is assumed to be available to both the attacker and defender. Later, the effects of the more realistic case of imperfect information is considered, since neither the attacker nor the defender can have complete knowledge of one another's state.

The attacker can use one or more combinations of the following types of attack. An attack consists of a string of one or more of the following classes:

interruption - Interruption is the termination of a service required by the network. Purposely overwhelming an application so that it cannot service other users is an example of interruption.

interception - Interception is obtaining information from the network useful for an attack. An example of interception is obtaining information from the network useful for an attack.

modification - Modification is a change of information in the network which weakens network security. Planting a virus is an example of modification.

fabrication - Fabrication is the construction of data for the purpose of weakening network security. This could include guessing passwords or building and sending invalid protocol data units.

Barriers exist to these forms of attack besides firewalls as shown in Table 2. Note that these defenses are effective independent of time. The simplified attack cost vector is shown in Equation (1). In this analysis vulnerability is quantified in units of time. For example, fabricating a password on a particular node will cost an attacker the amount of time which depends on the rate that new passwords can be generated, the number of accounts on the target node, and how well the passwords have been chosen.

TABLE 2

TIME INDEPENDENT (NON-POLLED) DEFENSES

Attack	Defense	Variable Name
interruption	improved design	id
interception	encryption	en
	authentication	au
	non-repudiation	nr
modification	signature	si
fabrication	signature	si

$$cf(p) = \begin{matrix} \\ \text{interruption} \\ \text{interception} \\ \text{modification} \\ \text{fabrication} \end{matrix} \begin{matrix} cf_i(p_i) \\ \begin{pmatrix} cf_1(p) \\ cf_2(p) \\ cf_3(p) \\ cf_4(p) \end{pmatrix} \end{matrix} \qquad (1)$$

Using the tool and analysis methods of the present invention, a network security analyst can allocate security safe-guards in order to minimize the entire network vulnerability, or to minimize the vulnerability from known attack points to particular targets.

As an attack takes place, the defender can use the tool to study the effectiveness of various strategies using actual network vulnerabilities, but within the safety of a simulation environment. The analysis tool can be used to determine the optimal location of services to be cut. The effect of concentrating on reducing specific vulnerability classes will be the focus, rather than cutting-off access to

entire network hosts that have been compromised. Also, by studying the past history of an attack, it will become apparent which vulnerability classes a particular attacker prefers to exploit.

From a fundamental network vulnerability flow viewpoint, the strategy of allocating safe-guards in combinations of serial and parallel strategies can be examined. Figure 12 shows Network Insecurity Path Assessment Tool analyzing an attack from host A to host B. In this case, the number of opportunities have been normalized into probabilities. Figure 13 shows the results as security safe-guards are removed. The solid line is the vulnerability of a single connection from the attacker to the defender having the same vulnerability flow as the links shown in Figure 12. Below a probability of 0.6 the diversity of vulnerability types helps to increase security, but interestingly, above 0.6 it does not.

Once an attack has been detected, the network command and control center can respond to the attack by repositioning security safe-guards and by modifying services used by the attacker. However, cutting-off services to the attacker also impacts legitimate network users and a careful balance must be maintained between minimizing the threat from the attack and maximizing services to customers. For example, various stages of an attack are shown in Figure 14. Since the allocation of security resources never changes throughout the attack, the vulnerability of the target increases significantly with each step of the attack.

Because vulnerabilities change over time, the network monitoring tool described quantifies the vulnerability of a system in terms of percent of patches which fail to have the correct signature (p_f), percent of files which are accessible to others besides the owner (p_r), and percent of passwords which can be guessed with a given password generation tool (p_g). Clearly, vulnerability checks such as these increase the security of the network. The effectiveness of a network monitoring strategy is quantified by both the

type of information gathered and the frequency that the information is updated. If the information is not updated frequently enough, an attacker may have penetrated network security and left before network security is aware of the situation.

In this analysis, a path with perfect security has a $cf_i(p_i) \rightarrow \infty$, and a path with no security has a $cf_i(p_i) \rightarrow 0$. The vulnerability of a path is defined as the inverse of the $cf_i(p_i)$. An estimate of the effectiveness of the monitoring system is based on a profile of network security attacks on the Internet and the following parameters: time to monitor patches, Trojan horses, passwords, and any other vulnerabilities (t_s), the attack rate is Poisson and the attack duration is exponential with average a_r, and monitoring is performed every λ_m seconds. The average attack rate, based on Internet incident reports from an anonymous site for a six year period, is five attacks per month. Also, the Defense Information Systems Agency has determined by experimental means that only 0.7% of incidents are actually reported. Thus the probability of detecting an attack while the attack is taking place along path *i* is shown in Equation (2), and the results are graphed in Figure 15 with $a_r = 5/(0.007)(30)(24)$, the y-axis is P[*detect*], and the x-axis is $\lambda_m + t_s$.

$$P_i[\text{detect}] = 1 - e^{-a_r \frac{1}{\lambda_m + t_s}} \qquad (2)$$

Thus, for each path in the network security vulnerability chain, the cost to the attacker is the probability of being detected multiplied by the cost function that the additional monitoring provides. Thus the total cost function is shown in Equation (3).

$$cf_i(p_i) = \left(1 - \prod_{n=0}^{i} \overline{P_n[detect]}\right) (p_g + p_o + p_f) + (id + en + au + si) \qquad (3)$$

Figure 16 shows the increase in probability of detection as an intruder passes through multiple systems where each system has its own independent detection system.

The tool has served as experimental validation of a variety of techniques to analyze a communications network for vulnerabilities. It can be taken a step farther, however, by adding the capability of automatically determining the placement of security safeguards based on predetermined cost limitations.

Let S be the placement of security safeguards (*e.g.*, encryption, firewall, authentication), and V be the vulnerability. Let C be the cost of the safeguards, and L be some threshold to the acceptable cost. The Object Function (4) sets up the optimization problem:

$$\min V(S) \quad \text{subject to } C(S) < L. \tag{4}$$

Network security tends to hamper the effectiveness of the network to legitimate users. Taking this into account, let CS represent the network service to legitimate users of the network, with a minimum accepted quality, Q, and V(A) be the vulnerability of the network to a particular attacker, A. The Object Function (5) sets up the optimization problem:

$$\min V(S,A) \quad \text{subject to } CS > Q, \; C(S) < L. \tag{5}$$

The tool is written in Sun Java with JDK 1.2. Secanal is the main Java application. The use of the tool will now be explained in detail.

Enter "java Secanal" to begin the application. A large button should appear as shown in Figure 17. The complete command line arguments are "java Secanal [-b filename][-f filename][-s nodenumber][-l layout]". The -b option loads an

IW file explained *infra*, the -f. option loads a GML file explained *infra*, the -s option begins the applications with a given node already selected, and the -l option is the label of a menu item to be executed upon start-up.

Click on Start Security Analysis to bring up the screen shown in Figure 18. Note that at any time nodes and edges can be added, deleted, or modified in a vulnerability graph in order to test "what if" scenarios. The toggle switches in the upper left allow Nodes and Edges to be created or selected. Clicking on the graph in the mode shown in Figure 18 will create a new Node.

The graph area is three-dimensional; the view angle can be changed by clicking within the viewing angle area in the lower left of the screen. An "x" will be placed in the view area indicating the corresponding angle of θ and ϕ. In addition the scale can be changed. The viewing offset is required because the graph area is larger than what is displayed within the window. Click on File from the menu along the top of the screen. The window shown in Figure 19 will appear. Open the gmi directory and open example.gml. GML is a standard notation for representing graphs and can be read by other graph applications such as graphlet (http://www.uni-passau.de/graphlet/).

Select example.gml and the example graph should be loaded as shown in Figure 20. The nodes represent vulnerability classes, the edges represent the number of opportunities to advance from one vulnerability class to another.

There are two main algorithms that can be run; the first is a probabilistic analysis and the second is a maximum flow analysis. First, the probabilistic analysis will be discussed. Select a node to be the target of the attacked by clicking on the Select Nodes toggle button. Then select a node (*e.g.*, hosts C Vuln 4). A white cross hair should appear over the node to indicate it has been selected. Choose Algorithms; choose Security Analysis Models and finally choose probabilistic analysis. A text window shown in Figure 21

should appear which states the probability of successful attack followed by the result graph shown in Figure 22. The result graph shows the most probable path of attack highlighted. The edge values are normalized between 0 and 1 to represent the probability of an attacker choosing that path.

The analysis can also be run using the maximal flow algorithm as follows: Choose File and Open GML. Then choose the gml directory and choose the example.gml file. The graph window should appear as shown in Figure 20. Select Hosts C Vuln 4 again and choose Algorithms Security Analysis Models and Max Flow Analysis. The text window shown in Figure 23 should appear as well as the graph results shown in Figure 24. The edge values have been changed to show the maximum flow along each edge towards a target node. In this case there is a flow of 1.0 and a flow of 5.0 which can reach the target node. Now choose File and Exit This Window in order to close the window in Figure 24. The original window should still be open.

One method of adding security may be to partition the vulnerabilities so that paths do not exist across the vulnerability chain. One method to determine how to partition the chain is to determine the articulation points. These are single nodes which if removed from the graph will partition the graph into multiple disconnected subgraphs. In order for this to work the graph must be undirected. Choose Properties and Directed. This will toggle the graph in undirected mode; the arrows will disappear from all the edges. Next choose algorithms and Biconnectivities and choose Find Articulation Points. A window as shown in Figure 25 will appear. In order to identify the node number on the graph, select a node and the node number and position will appear along the top of the main window.

The tool is also capable of executing other commands and controls such as automated node layout, importing and exporting vulnerability graphs, filtering, grouping, and automatically adding an attack node.

The options labeled Tree and Spring under Algorithms are different methods for displaying the graph node positions. For example, select a node to be the root of the tree and then select Tree and Tree Down. Figure 26 shows the result of selecting the attacker as the root in choosing Tree Down. The Spring button attempts to layout the nodes such that edges modeled as springs and the nodes are positioned such that the energy between the springs is minimized.

An optional argument to Secanal is -b filename.filename is the complete path and file in which data collected from the IW agents are collected. The file format is similar to the following:

```
Start up server on port 1661
Server listening on port 0 using fileno 5
     Server.pl: Boss send us message of: read_all_data
host/HostA
IW.pl:handle_request
read relationship Relationships
read os PERM.Solaris.2.5.1-SunOS/5.5.1
Found OS SunOS/5.5.1
IW.pl.handle_request:exit
Server.pl: Boss send us message of: report_all_files
host/HostA
IW.pl:handle_request
ID:Vulnerability/*/991
NAME:Vulnerability/hostb/14
          data[count]=0
          data[name]=Vulnerability/hostb/14
          data[type]=Trojan
          data[vector]=Directory=HASH(0x51ca54)
          data[victim]=Account=HASH(0x460fc8)
          data[attacker]=Account=HASH(0x46de24)
          Reference(Account)=(account/hostb/root)
```

When importing vulnerabilities, there can exist many thousands of fundamental vulnerabilities which can overwhelm this tool and the user if they are displayed individually.

However, vulnerabilities can be grouped based on Host, Id, Type, and a combination of Host and Type. This means that only one vulnerability will appear for each host, vulnerability identifier, vulnerability type, or a combination of host and type. Choose Algorithms and Filter Nodes and then one of the above filter types. Once this has been done, the tool will remember that filter and apply it each time vulnerability data is imported. To import vulnerability data, choose Algorithms and Import and Update Security Model. Note that imported vulnerability data updates the graph. For example, if a vulnerability graph is already displayed on the screen then importing vulnerability data will add the data to the graph.

There are two methods for exporting vulnerability graph data. The first is to save the graph in a GML file. This can be done choosing File and Save As GML. The second export format is a format readable by Mathematica. Choose Algorithms and Export Data and Convert to Mma. The data will be saved in a directory named mma assumed to exist under the current directory in which Secanal resides. The files are Adj.mma (Adjacency Matrix), Arc.mma (Edge Index Matrix), Cons.mma (Constraint Matrix), Flow Adj.mma (Adjacency Matrix with Flow values), and Inc.mma (Incidence Matrix). In addition to the above files, Adj.mo and FlowAdj.mo are generated in the mma directory. These files contain the data only arranged in row-column format.

Vulnerability nodes can be grouped together in a single node as follows. Choose Algorithms and Group Nodes and then choose one of Host, Id., Type, Host and Type, or common Child. In Figure 27, a vulnerability graph is shown before nodes have been grouped. After choosing Group and Host, the graph in Figure 28 is created. Choosing Edit and Group Control-seeNode brings up the menu shown in Figure 29 which can be used to create or remove selected groups.

In order to facilitate adding an attack node, select the node to which the attacker should be adjacent and then choose Algorithms and Security Analysis Models and Add Attack Point. An attack node will be automatically created and

attached directly to the selected node. Note that the attacking node must be labeled "Attacker" in order to be recognized as the attacker in the algorithms.

The tool is also capable of manually editing vulnerability graphs in order to analyze "what if" scenarios.

As an example, load the example gml graph as explained *supra*. Choose the Select Nodes button. The goal of this example will be to move the attack node from Host A Vulnerability 1 to Host B Vulnerability 2. This will demonstrate how to delete and create nodes and create and modify edges. Select the Attack and then choose Edit and Delete Selected Items. Both the Attack node and its adjacent edge will be removed. Select Create Nodes. Click on the graph near Host B vulnerability 2. This will create a new node as shown in Figure 30.

Choose Select Nodes and double-click on the new node. The window shown in Figure 31 should appear. Enter Attacker for the label then choose apply. The label should be changed from a node number to "Attacker."

Next choose Create Edges and select the Attacker node. The new edge should follow the cursor as it moves. Select Host B Vulnerability 2. An arrow should appear connecting the two nodes and directed from the Attacker to the vulnerability node. Choose Select Edges and double-click on the new edge. The window shown in Figure 32 should appear. Enter a value for the label and choose Accept. The graph should appear as shown in Figure 33.

Select Host C Vuln 4 and run the probabilistic analysis. The textural result is shown in Figure 34 and the graphical result is shown in Figure 35. Notice that the probability of successful attack is 0.226 in this analysis and 0.729 in the previous case. This should be expected since the path of most probable attack is longer in this analysis.

The present invention is capable of displaying the results of the vulnerability analysis in a number of ways. As seen above, the results can be displayed either graphically or texturally. In addition to the 2-dimensional graphical

analysis, the invention provides a 3-dimensional topological display of the vulnerabilities in the network. This technique allows easy identification of the security weaknesses within the network by displaying a clear 3-dimensional view of mountain peaks and valleys super-imposed upon the network node layout. The node layout can be grouped by physical location or by type. The invention then allows one to examine the impact upon the entire network of the location of various security safeguards within the network, thus facilitating a security cost-benefit analysis and optimizing the placement of security safeguards. Because it is difficult to know from where an attack will take place, the flow from every node to every other node is calculated. A contour is drawn based on the accumulated vulnerability and the distance from each node. An example contour is shown in Figure 36. The contour shows the rate of change of vulnerability as one moves through the network. The resulting topological map or an alternative density plot graph provides quick visual information indicating where vulnerabilities lie. This topological display aspect of the invention was written and implemented in *Mathematica*.

The overall vulnerability of network is represented by a directed graph of all vulnerability chains or paths that an attacker could use to invade the network. The present invention allows easy identification of the security weaknesses of the entire network to specific threats by identifying the path of least resistance to the attacker's target. The invention then allows one to examine the impact of locating various security safeguards within the network, thus facilitating a security cost-benefit analysis and optimizing the placement of security safeguards. Finally, one embodiment of the present invention displays the results of the analysis in both a 2-dimensional and 3-dimensional (topological) display.

While only certain preferred features of the invention have been illustrated and described, many modifications and changes will occur to those skilled in the

art. It is, therefore, to be understood that the appended claims are intended to cover all such modifications and changes as fall within the true spirit of the invention.

We Claim:

1. A method of analyzing multiple computer network vulnerabilities, comprising:

gathering vulnerability data from one or more hosts within the network; and

generating a directed graph from the gathered vulnerability data where nodes in the directed graph represent vulnerabilities within the network, and paths between nodes are defined as edges, and the edges represent probability values associated with moving from one vulnerability to another.

2. The method of claim 1, wherein all edges between the same two nodes are normalized into a single probability value.

3. The method of claim 2 further comprising:

multiplying probabilities of paths in series from a source node to a destination node;

adding probabilities of paths in parallel from the source node to the destination node; and

determining from the multiplication and addition the probabilities of all routes from the source node to the destination node.

4. The method of claim 3, wherein a most probable route between the source node and the destination node represents a most vulnerable attack path.

5. The method of claim 2, further comprising:

using an optimization technique to determine maximum insecurity flow from a source node to a destination node, wherein the optimization technique maximizes flow from the source node while conserving flow through intermediate edges of the graph.

6. The method of claim 2, further comprising:

finding a minimum number of nodes that can be

deleted from the graph resulting in a partitioning of the graph into at least two isolated sections.

7. The method of claim 2, further comprising:
displaying the directed graph.

8. The method of claim 7, wherein the display comprises a two-dimensional graph displayed on a monitor.

9. The method of claim 7 wherein the display comprises textural information displayed on a monitor.

10. The method of claim 2 further comprising:
multiplying probabilities of paths in series from each node in the network to every other node in the network;
adding probabilities of paths in parallel from each node in the network to every other node in the network; and
determining from the multiplication and addition steps the probabilities of all routes from each node in the network to every other node in the network.

11. The method of claim 10, further comprising:
generating a topological display of the directed graph.

12. The method of claim 2, further comprising:
using an optimization technique to determine maximum insecurity flow from each node in the network to every other node in the network, wherein the optimization technique maximizes flow from each node while conserving flow through intermediate edges of the graph.

13. The method of claim 1, further comprising:
determining a placement of security safeguards based on predetermined cost limitations.

14. The method of claim 13, further comprising:

determining the placement of security safeguards based on a minimum accepted quality of network service to legitimate users of the network.

15. A system for analyzing multiple computer network vulnerabilities, comprising:

a processor that includes computer-executable instructions for gathering vulnerability data from one or more hosts within the network; and generating a directed graph from the gathered vulnerability data; wherein nodes in the directed graph represent vulnerabilities within the network, and paths between nodes are defined as edges; and wherein the edges represent probability values associated with moving from one vulnerability to another.

16. The system of claim 15, wherein the processor further includes computer-executable instructions for multiplying probabilities of paths in series from a source node to a destination node; adding probabilities of paths in parallel from the source node to the destination node; and determining from the multiplication and addition the probabilities of all routes from the source node to the destination node.

17. The system of claim 15, further comprising:

a monitor for displaying the directed graph.

18. A computer readable storage medium, comprising computer-executable instructions for:

gathering vulnerability data from one or more hosts within a computer network; and

generating a directed graph from the gathered vulnerability data, wherein nodes in the directed graph represent vulnerabilities within the network, and paths between nodes are defined as edges, and wherein the edges represent probability values associated with moving from one vulnerability to another.

100

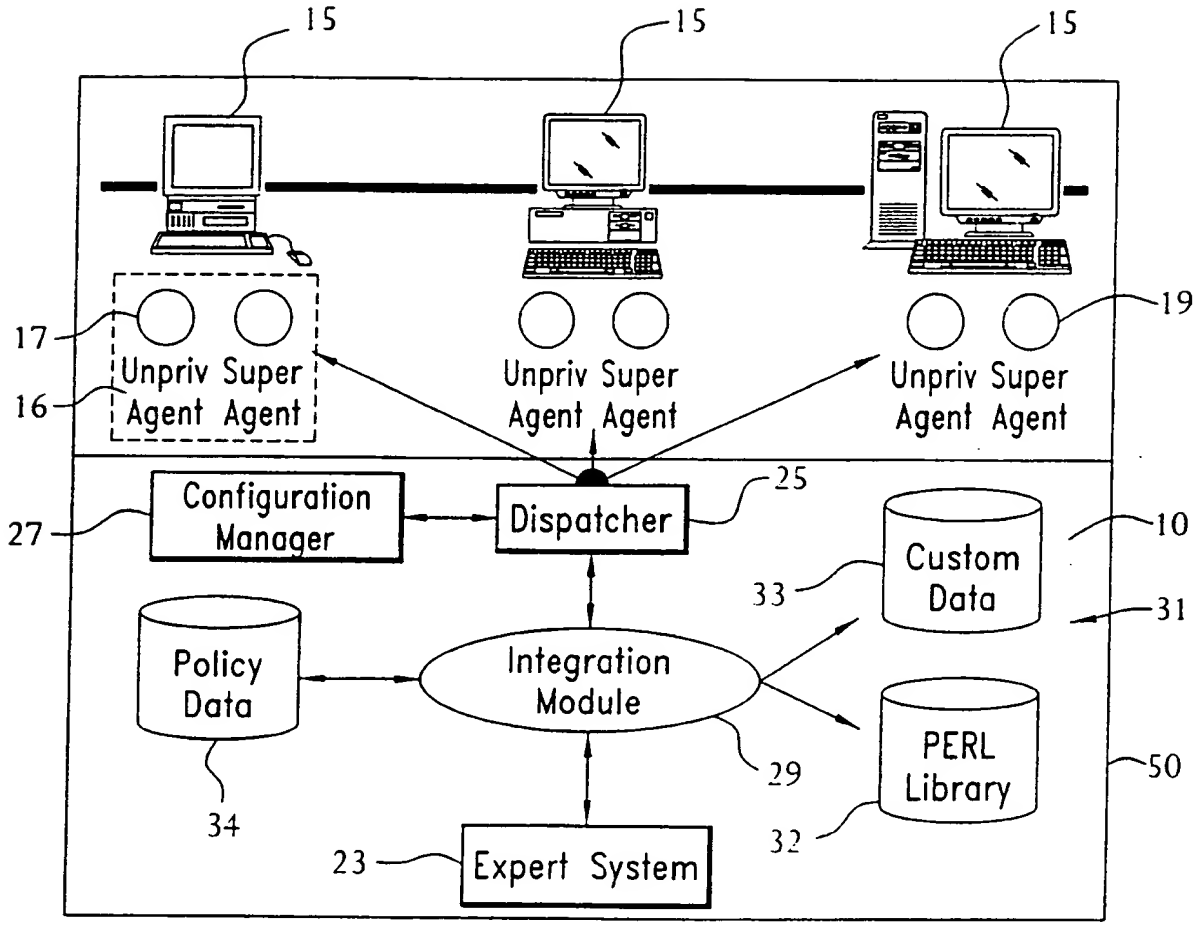

15
15
15
17
16
Unpriv Super Agent Agent
Unpriv Super Agent Agent
Unpriv Super Agent Agent
19
27
Configuration Manager
Dispatcher
25
10
33
Custom Data
31
Policy Data
Integration Module
PERL Library
29
50
34
23
Expert System
32

FIG. 1

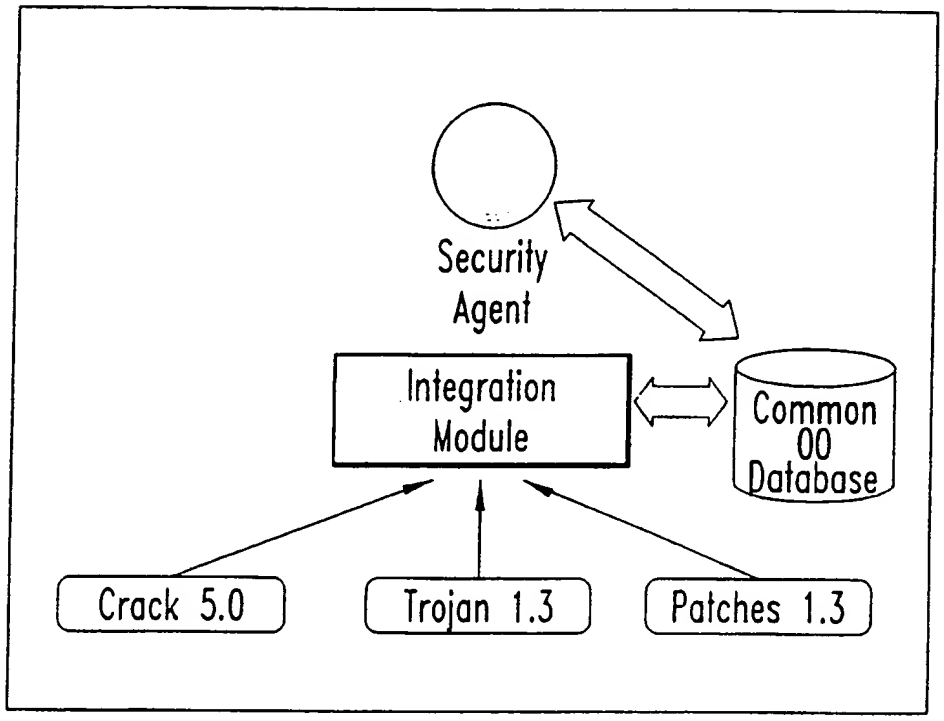

Security Agent
Integration Module
Common OO Database
Crack 5.0
Trojan 1.3
Patches 1.3

FIG. 2

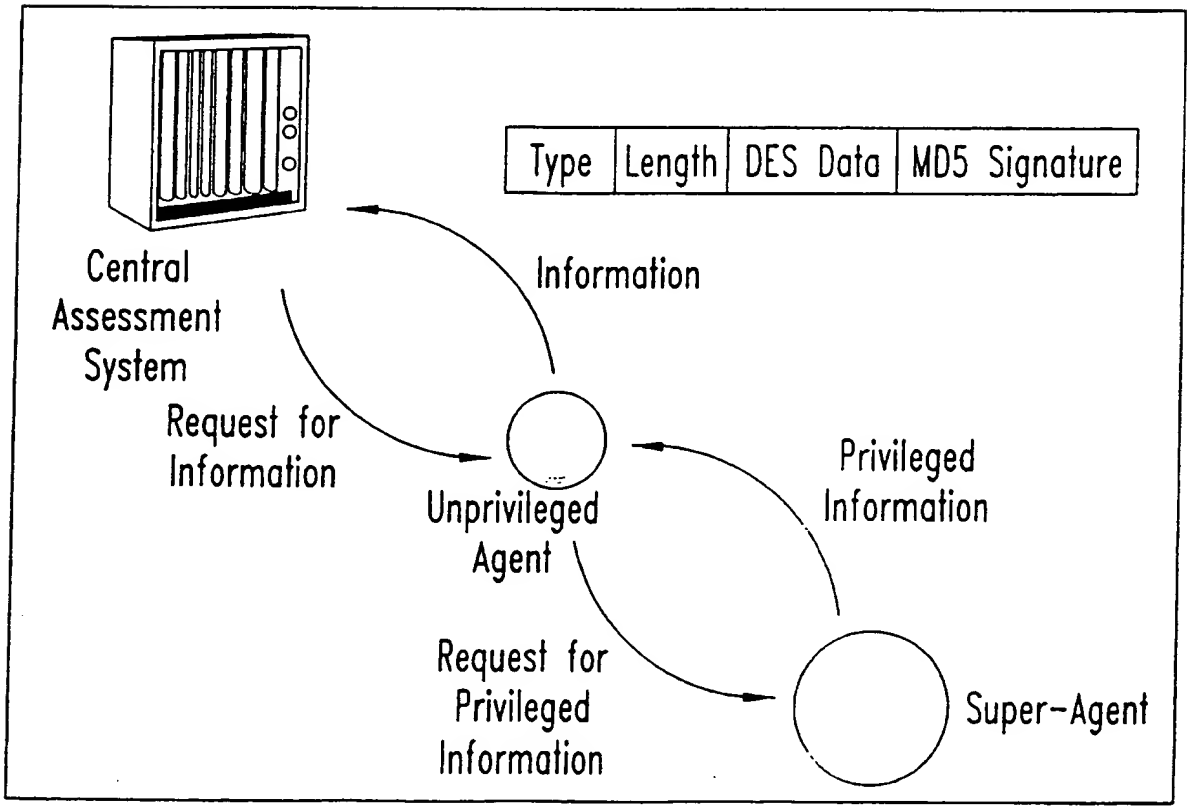

Type
Length
DES Data
MD5 Signature
Central Assessment System
Information
Request for Information
Unprivileged Agent
Privileged Information
Request for Privileged Information
Super-Agent

FIG. 3

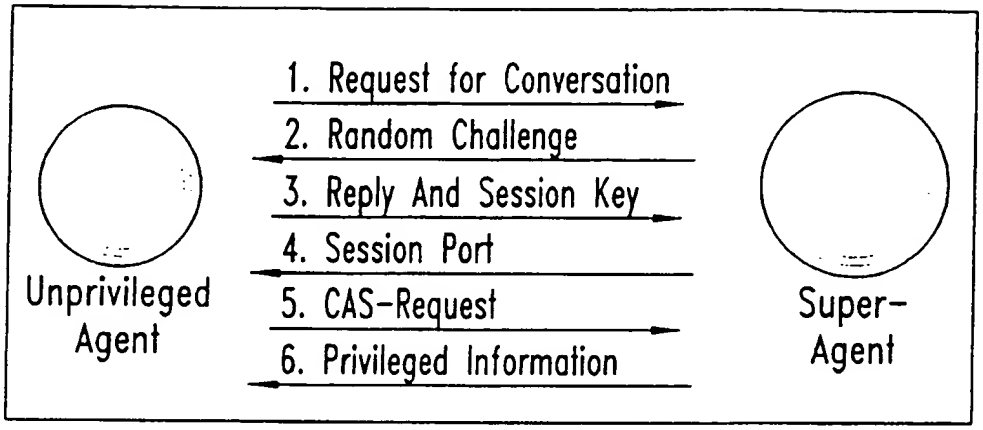

1. Request for Conversation
2. Random Challenge
3. Reply And Session Key
4. Session Port
5. CAS-Request
6. Privileged Information
Unprivileged Agent
Super-Agent

FIG. 4

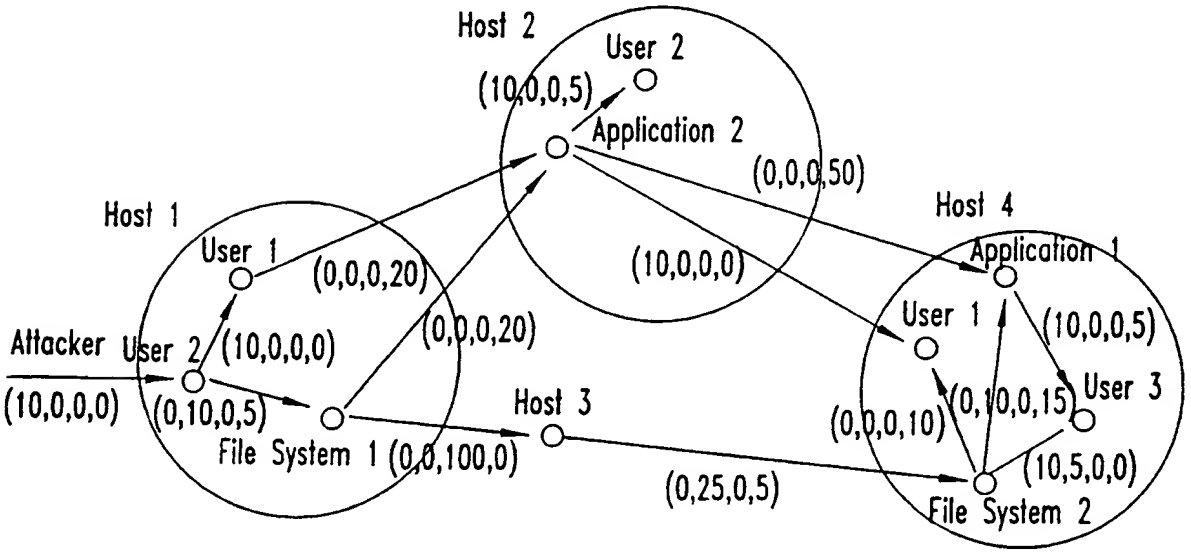

Host 2
User 2
(10,0,0,5)
Application 2
(0,0,0,50)
Host 1
User 1
(0,0,0,20)
(10,0,0,0)
Host 4
Application 1
Attacker
User 2
(10,0,0,0)
(0,0,0,20)
User 1
(10,0,0,5)
(10,0,0,0)
(0,10,0,5)
Host 3
(0,0,0,10)
(0,10,0,15)
User 3
File System 1
(0,0,100,0)
(10,5,0,0)
(0,25,0,5)
File System 2

FIG. 5

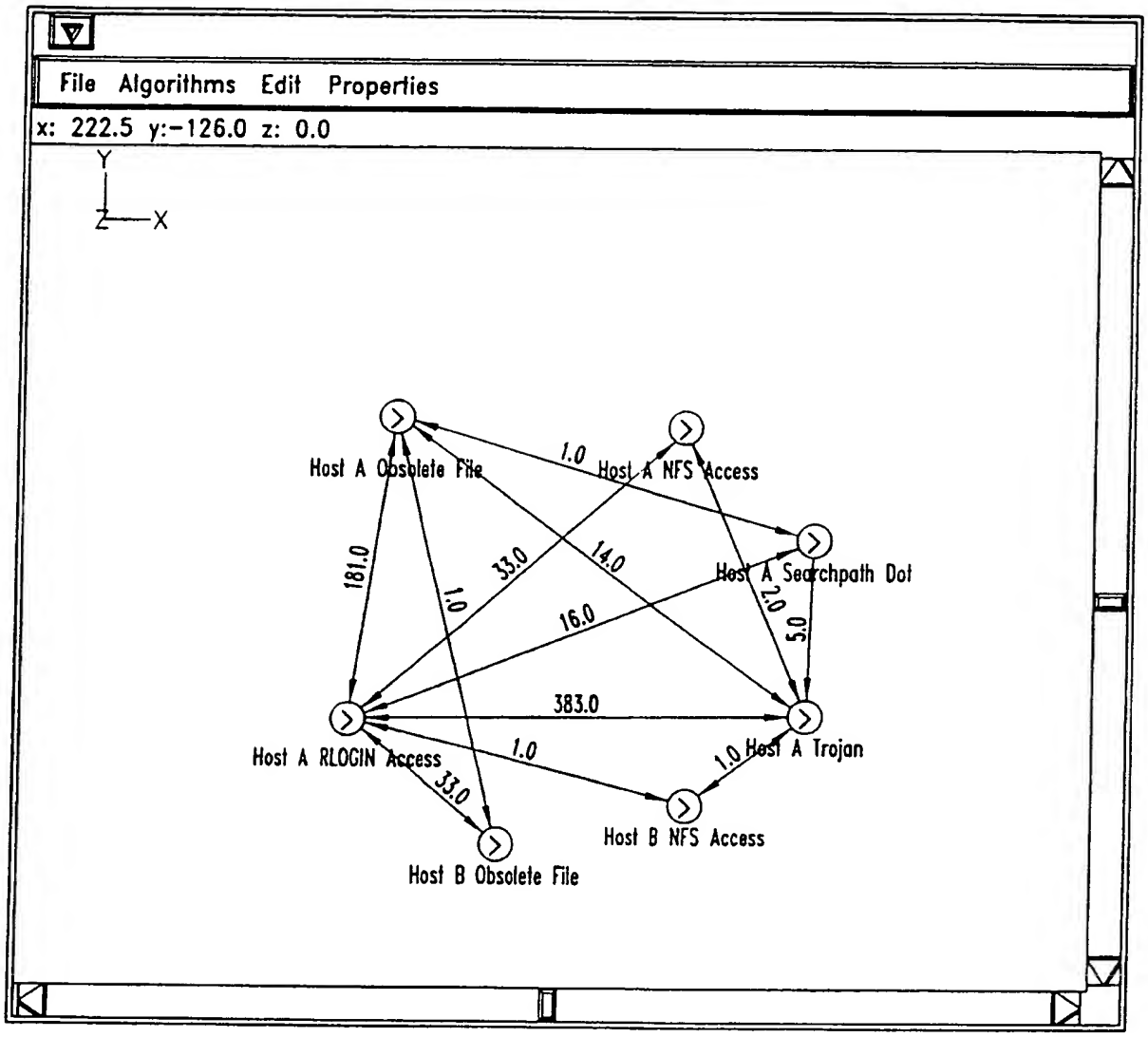

File Algorithms Edit Properties
x: 222.5 y:-126.0 z: 0.0
Y
Z
X
Host A Obsolete File
Host A NFS Access
Host A Searchpath Dot
Host A RLOGIN Access
Host A Trojan
Host B NFS Access
Host B Obsolete File
1.0
181.0
33.0
14.0
1.0
16.0
2.0
5.0
383.0
1.0
1.0
33.0

FIG. 6

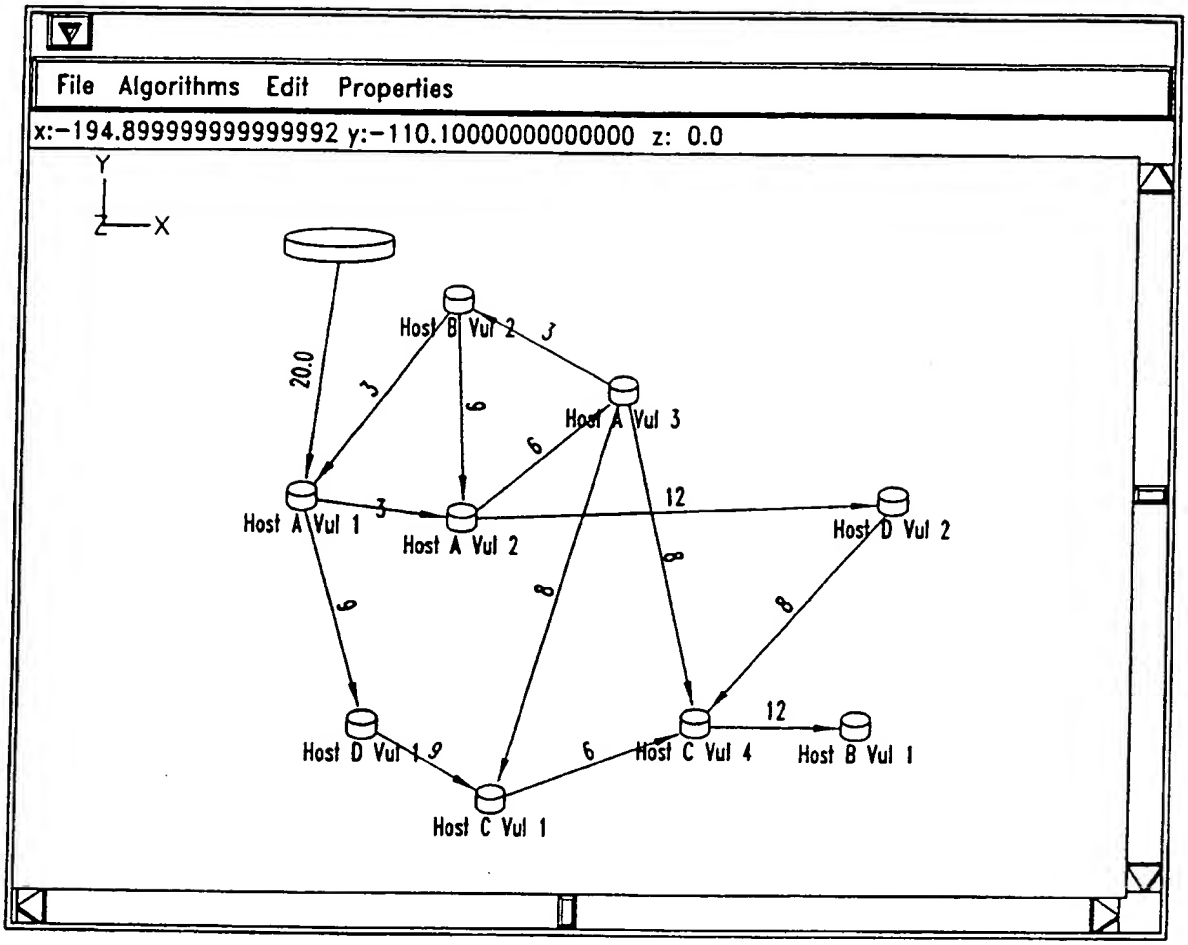

File Algorithms Edit Properties
x:-194.899999999999992 y:-110.10000000000000 z: 0.0
Y
Z
X
20.0
Host B Vul 2
3
3
6
Host A Vul 3
6
Host A Vul 1
3
Host A Vul 2
12
Host D Vul 2
6
8
8
8
12
Host D Vul 1
9
6
Host C Vul 4
Host B Vul 1
Host C Vul 1

FIG. 7

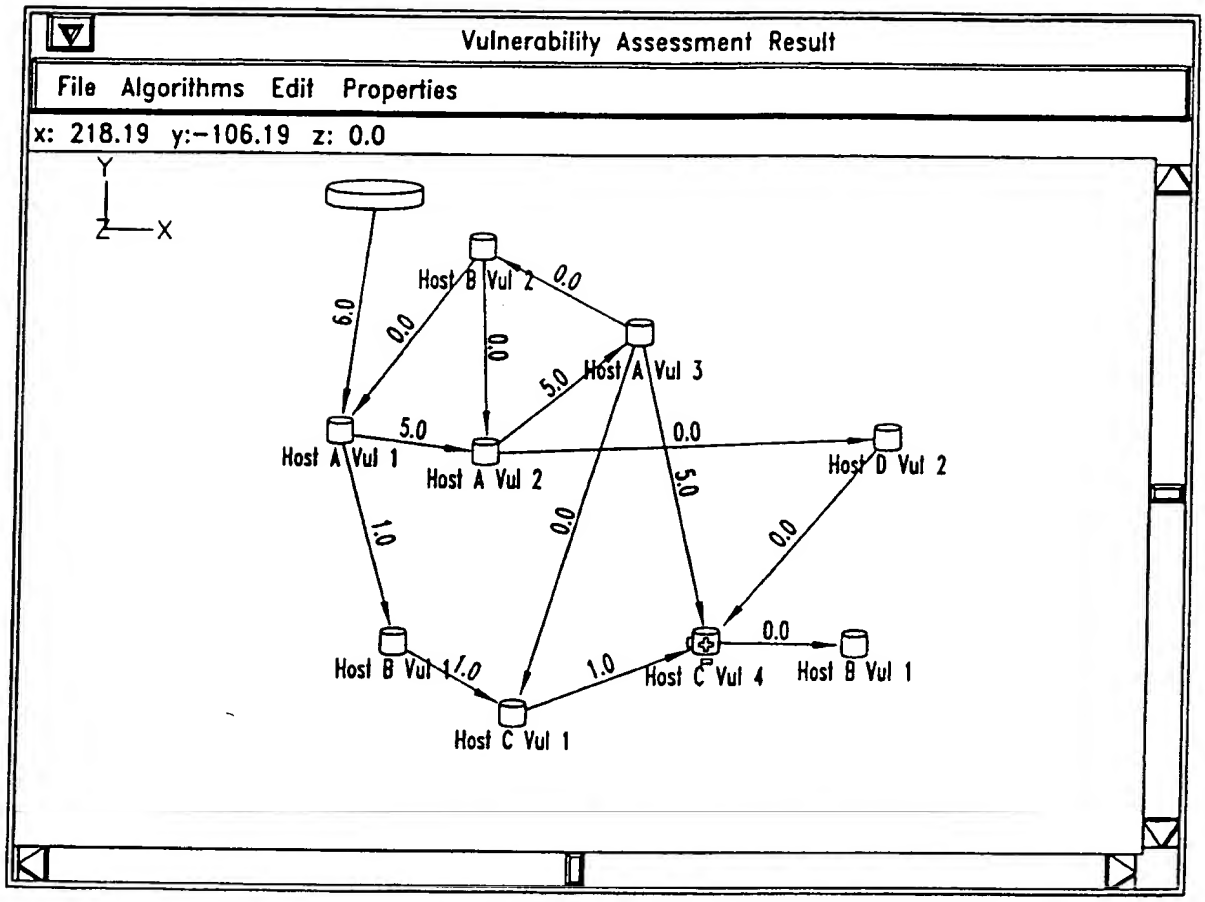

Vulnerability Assessment Result
File Algorithms Edit Properties
x: 218.19 y:-106.19 z: 0.0
Y
Z
X
Host B Vul 2
Host A Vul 3
Host A Vul 1
Host A Vul 2
Host D Vul 2
Host B Vul 1
Host C Vul 4
Host B Vul 1
Host C Vul 1
6.0
0.0
0.0
0.0
5.0
5.0
0.0
1.0
0.0
5.0
0.0
0.0
1.0
1.0

FIG. 8

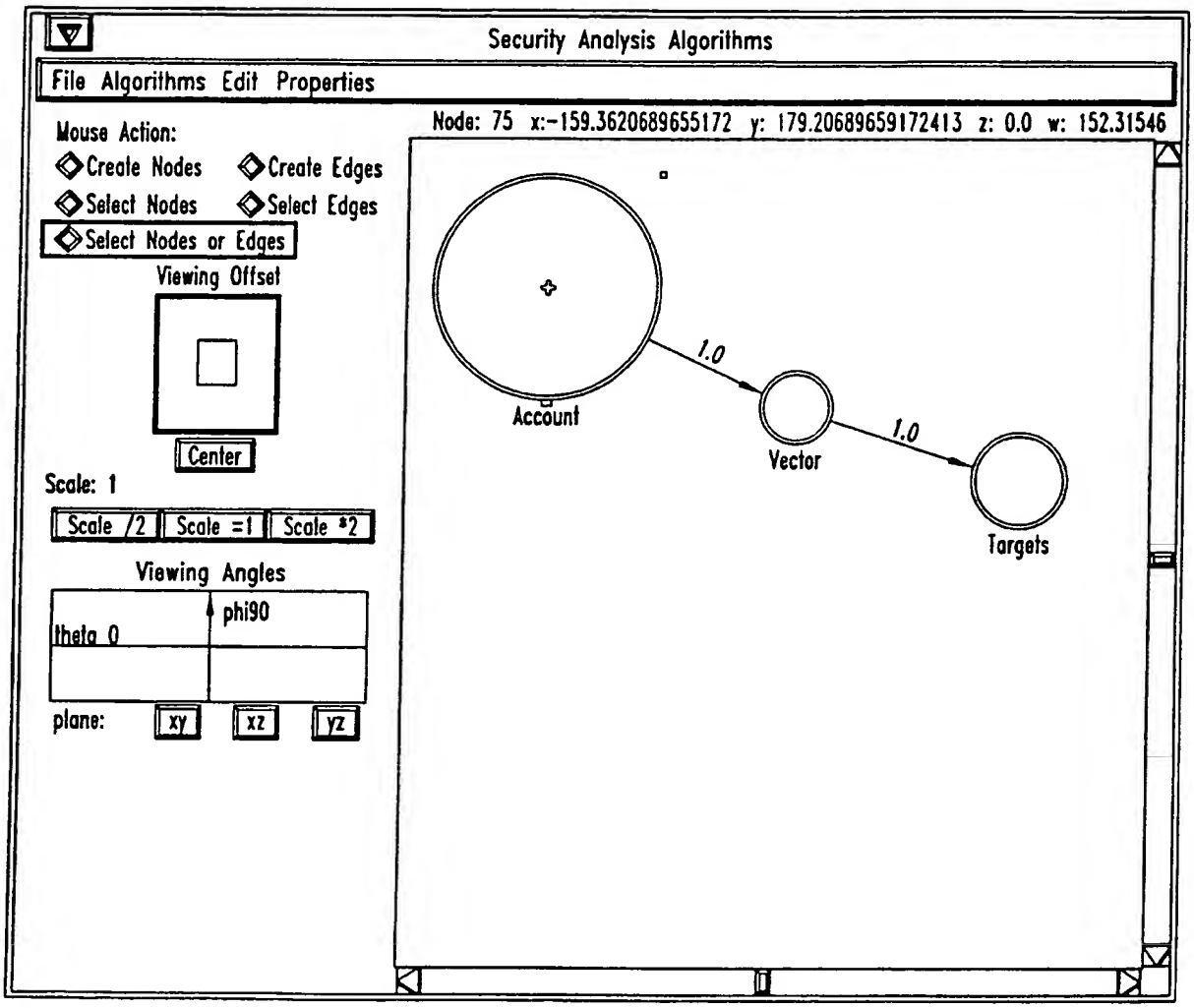

Security Analysis Algorithms
File Algorithms Edit Properties
Mouse Action:
Create Nodes
Create Edges
Select Nodes
Select Edges
Select Nodes or Edges
Viewing Offset
Center
Scale: 1
Scale /2
Scale =1
Scale *2
Viewing Angles
theta 0
phi90
plane:
xy
xz
yz
Node: 75 x:-159.3620689655172 y: 179.20689659172413 z: 0.0 w: 152.31546
1.0
1.0
Account
Vector
Targets

FIG. 9

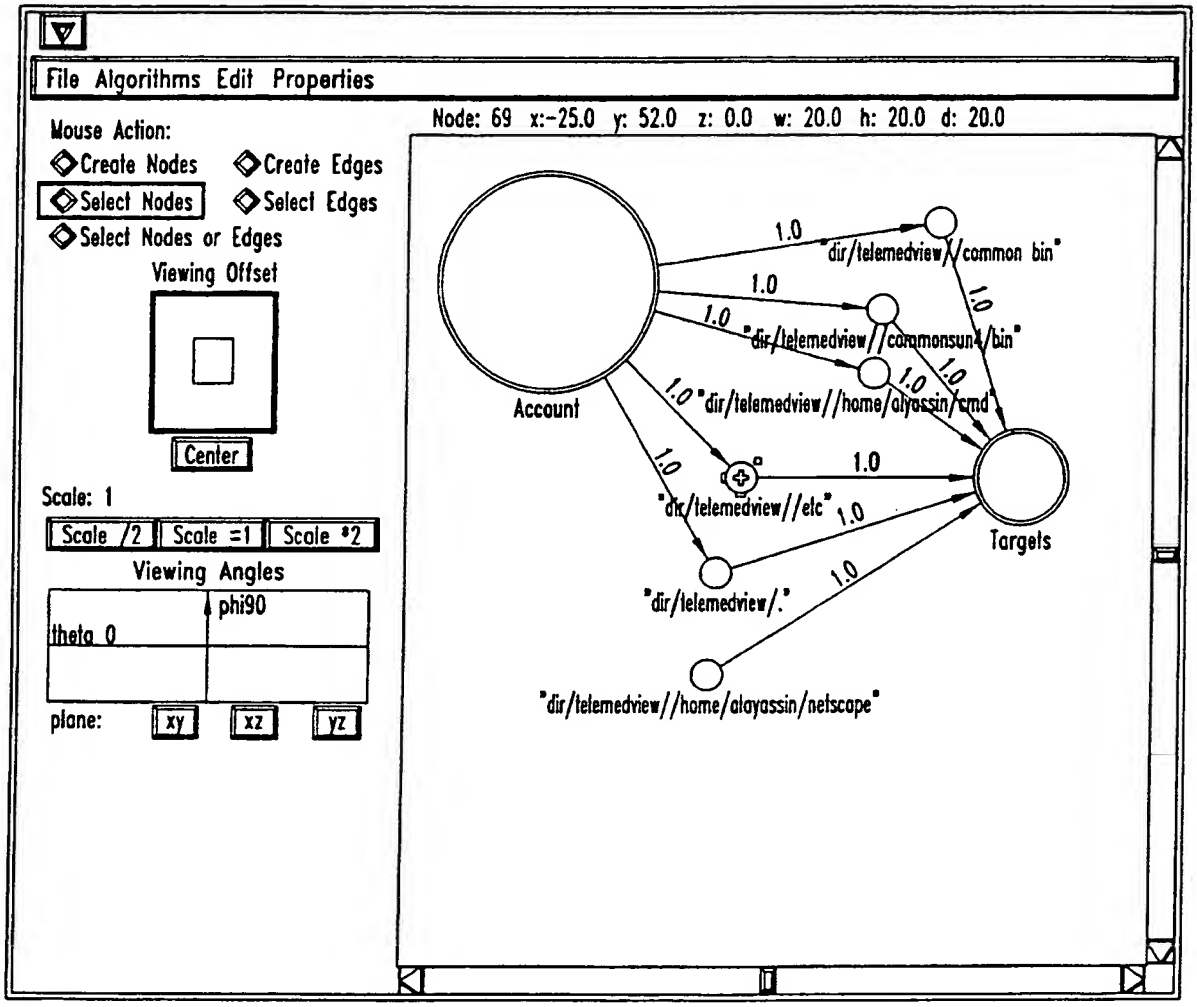

File Algorithms Edit Properties
Mouse Action:
Create Nodes
Create Edges
Select Nodes
Select Edges
Select Nodes or Edges
Viewing Offset
Center
Scale: 1
Scale /2
Scale =1
Scale *2
Viewing Angles
phi90
theta 0
plane:
xy
xz
yz
Node: 69 x:-25.0 y: 52.0 z: 0.0 w: 20.0 h: 20.0 d: 20.0
Account
Targets
1.0
"dir/telemedview//common bin"
"dir/telemedview//commonsun4/bin"
"dir/telemedview//home/alayassin/cmd"
"dir/telemedview//etc"
"dir/telemedview/."
"dir/telemedview//home/alayassin/netscape"

FIG. 10

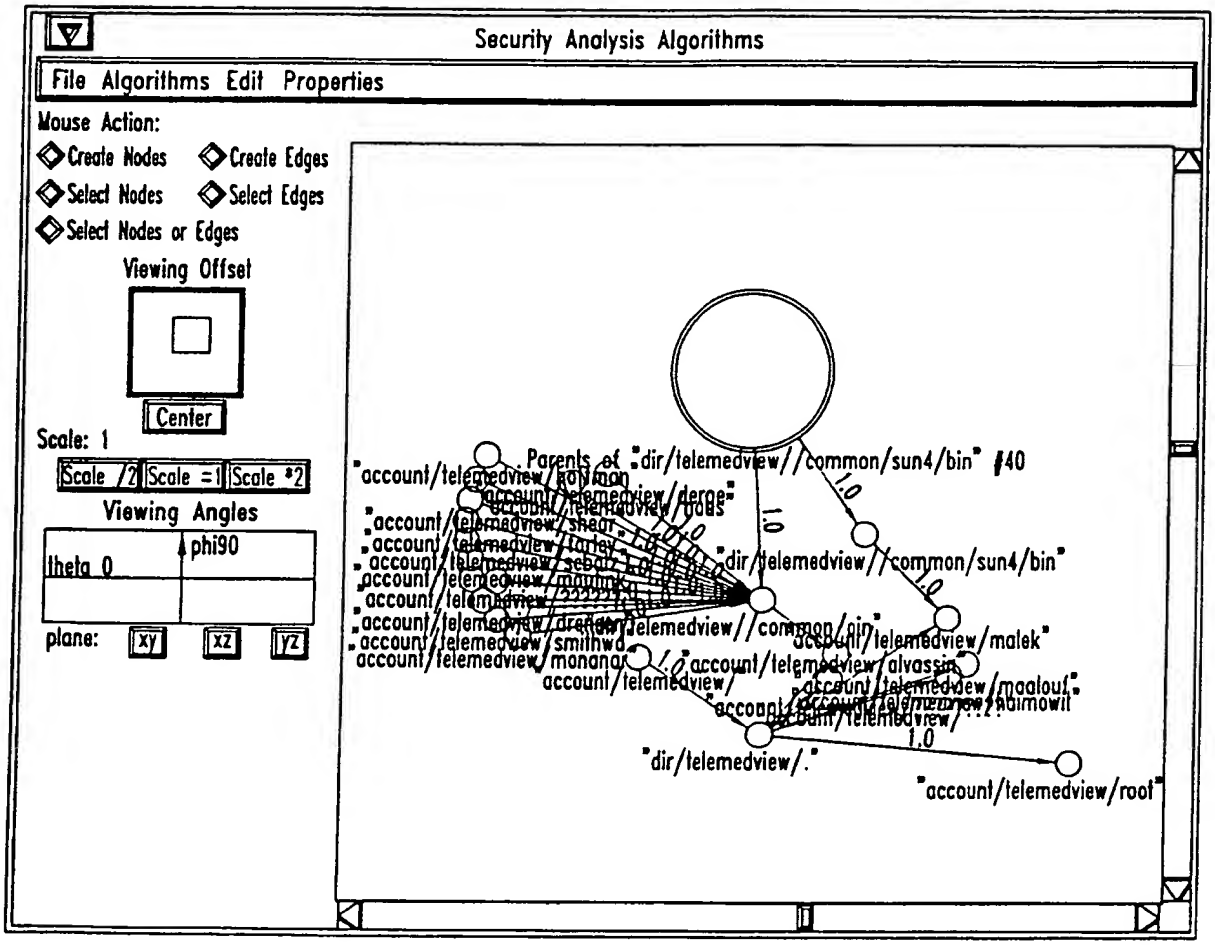

Security Analysis Algorithms
File Algorithms Edit Properties
Mouse Action:
Create Nodes
Create Edges
Select Nodes
Select Edges
Select Nodes or Edges
Viewing Offset
Center
Scale: 1
Scale /2
Scale =1
Scale *2
Viewing Angles
theta 0
phi90
plane:
XY
XZ
YZ
Parents of "dir/telemedview//common/sun4/bin" #40
"dir/telemedview//common/sun4/bin"
"dir/telemedview//common/sun4/bin"
"account/telemedview/malek"
"account/telemedview/alvassin"
"dir/telemedview/."
"account/telemedview/root"
1.0

FIG. 11

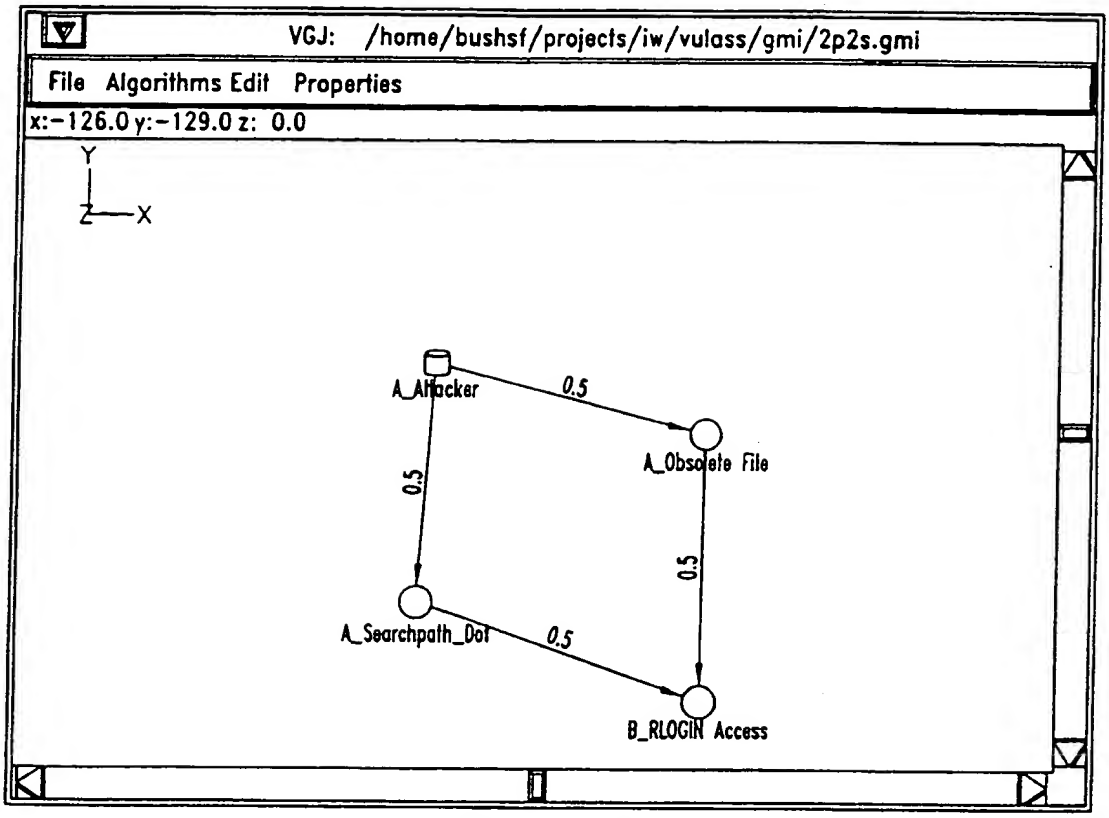

VGJ: /home/bushsf/projects/iw/vulass/gmi/2p2s.gmi
File Algorithms Edit Properties
x:-126.0 y:-129.0 z: 0.0
Y
Z
X
A_Attacker
0.5
A_Obsolete File
0.5
0.5
A_Searchpath_Dot
0.5
B_RLOGIN Access

FIG. 12

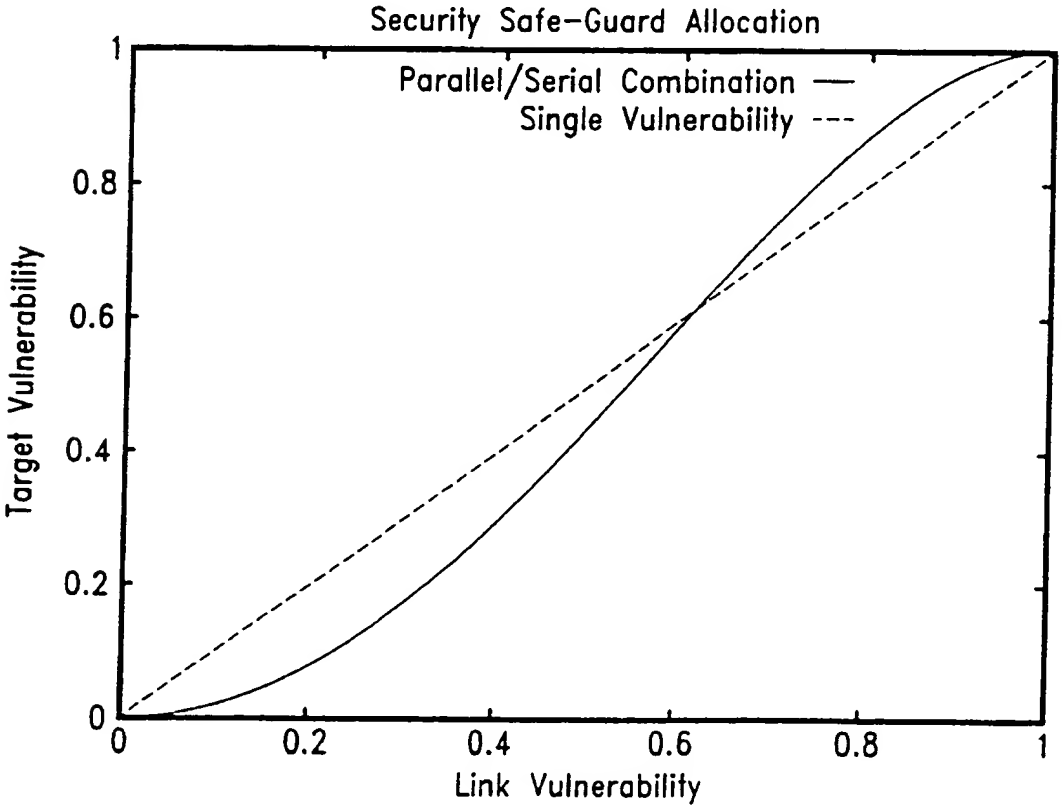

Security Safe-Guard Allocation
Parallel/Serial Combination
Single Vulnerability
Target Vulnerability
Link Vulnerability
0
0.2
0.4
0.6
0.8
1

FIG. 13

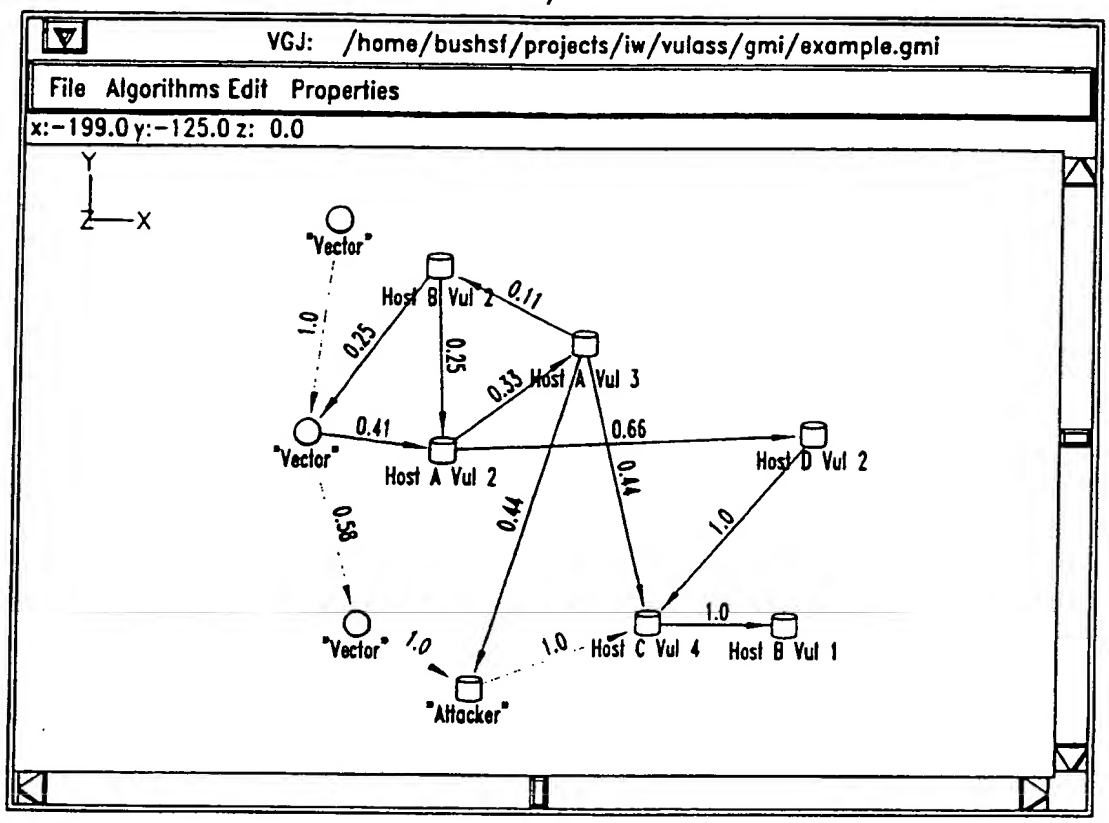

VGJ: /home/bushsf/projects/iw/vulass/gmi/example.gmi
File Algorithms Edit Properties
x:-199.0 y:-125.0 z: 0.0
Y
Z
X
"Vector"
Host B Vul 2
0.11
1.0
0.25
0.25
0.33
Host A Vul 3
"Vector"
0.41
0.66
Host A Vul 2
Host D Vul 2
0.44
0.44
0.58
1.0
"Vector"
1.0
1.0
Host C Vul 4
1.0
Host B Vul 1
"Attacker"

FIG. 14

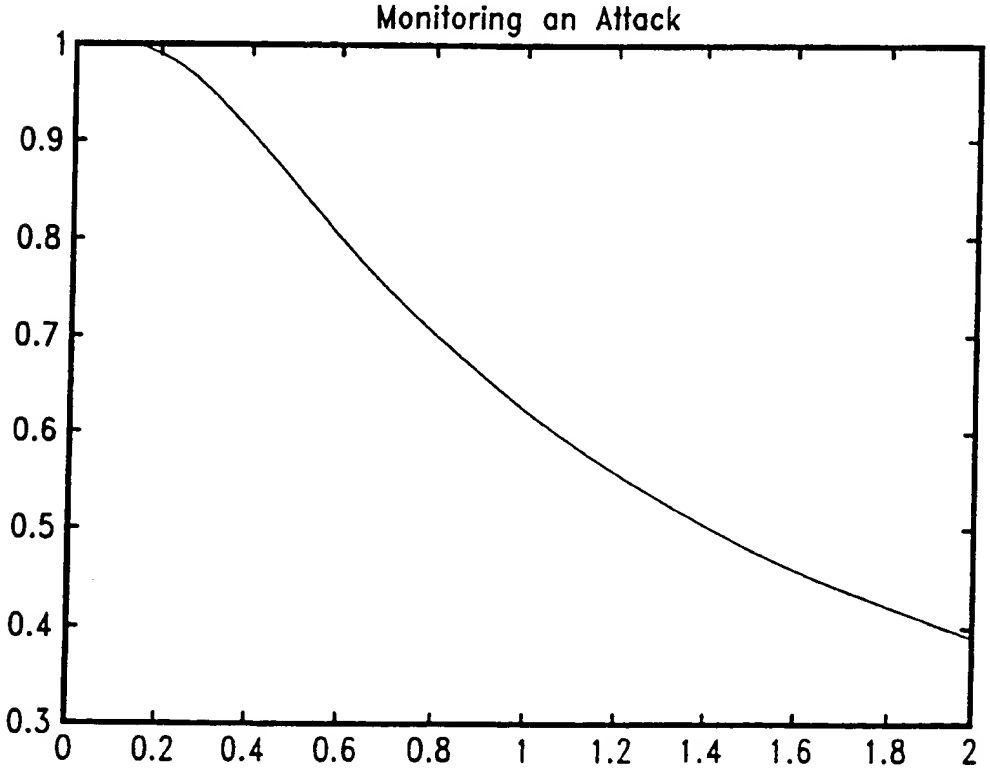

Monitoring an Attack
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0
0.2
0.4
0.6
0.8
1
1.2
1.4
1.6
1.8
2

FIG. 15

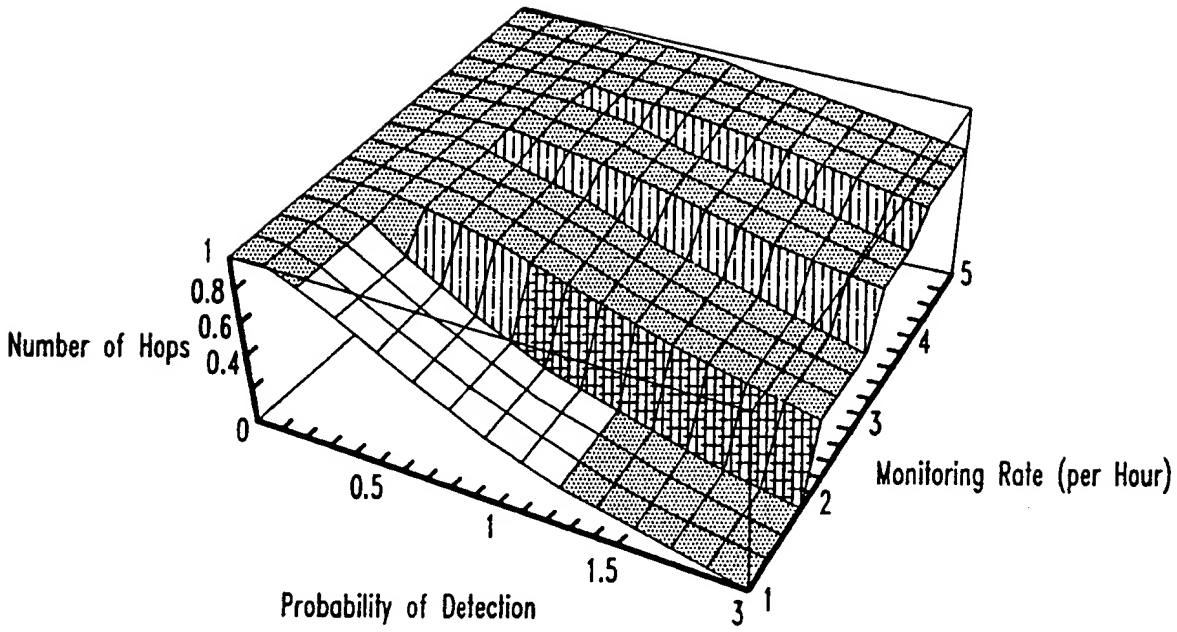

Number of Hops
1
0.8
0.6
0.4
0
0.5
1
1.5
Probability of Detection
3
1
2
3
4
5
Monitoring Rate (per Hour)

FIG. 16

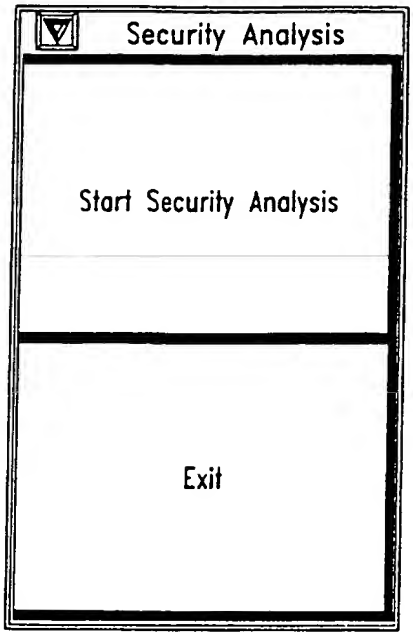

Security Analysis
Start Security Analysis
Exit

FIG. 17

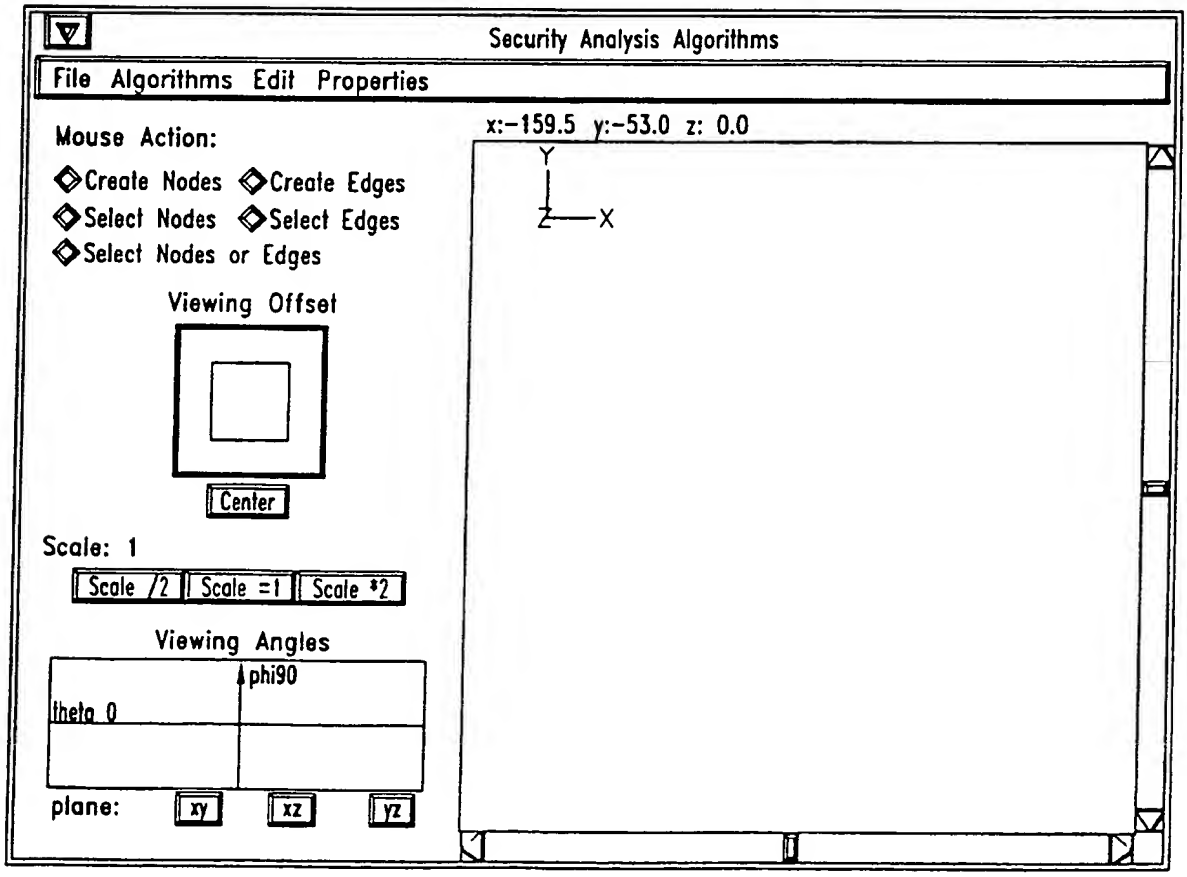

Security Analysis Algorithms
File Algorithms Edit Properties
Mouse Action:
Create Nodes
Create Edges
Select Nodes
Select Edges
Select Nodes or Edges
Viewing Offset
Center
Scale: 1
Scale /2
Scale =1
Scale *2
Viewing Angles
phi90
theta 0
plane:
xy
xz
yz
x:-159.5 y:-53.0 z: 0.0
Y
Z
X

FIG. 18

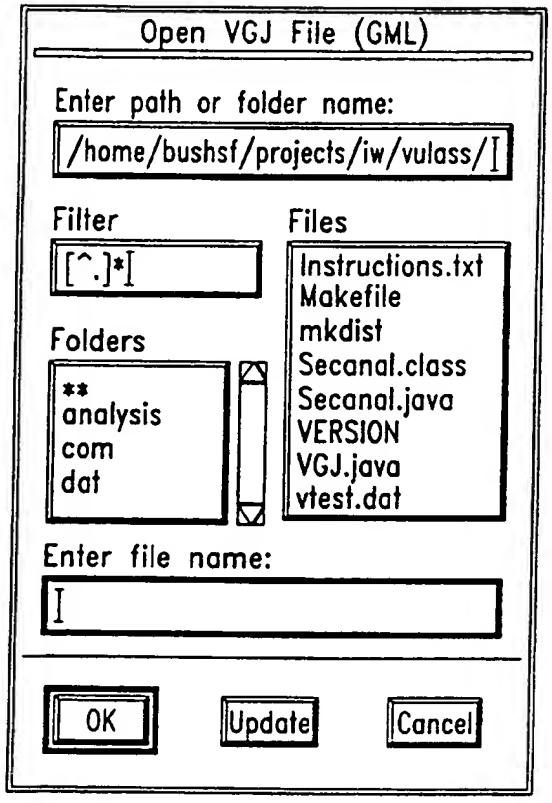

Open VGJ File (GML)
Enter path or folder name:
/home/bushsf/projects/iw/vulass/
Filter
[^.]*
Files
Instructions.txt
Makefile
mkdist
Secanal.class
Secanal.java
VERSION
VGJ.java
vtest.dat
Folders
**
analysis
com
dat
Enter file name:
OK
Update
Cancel

FIG. 19

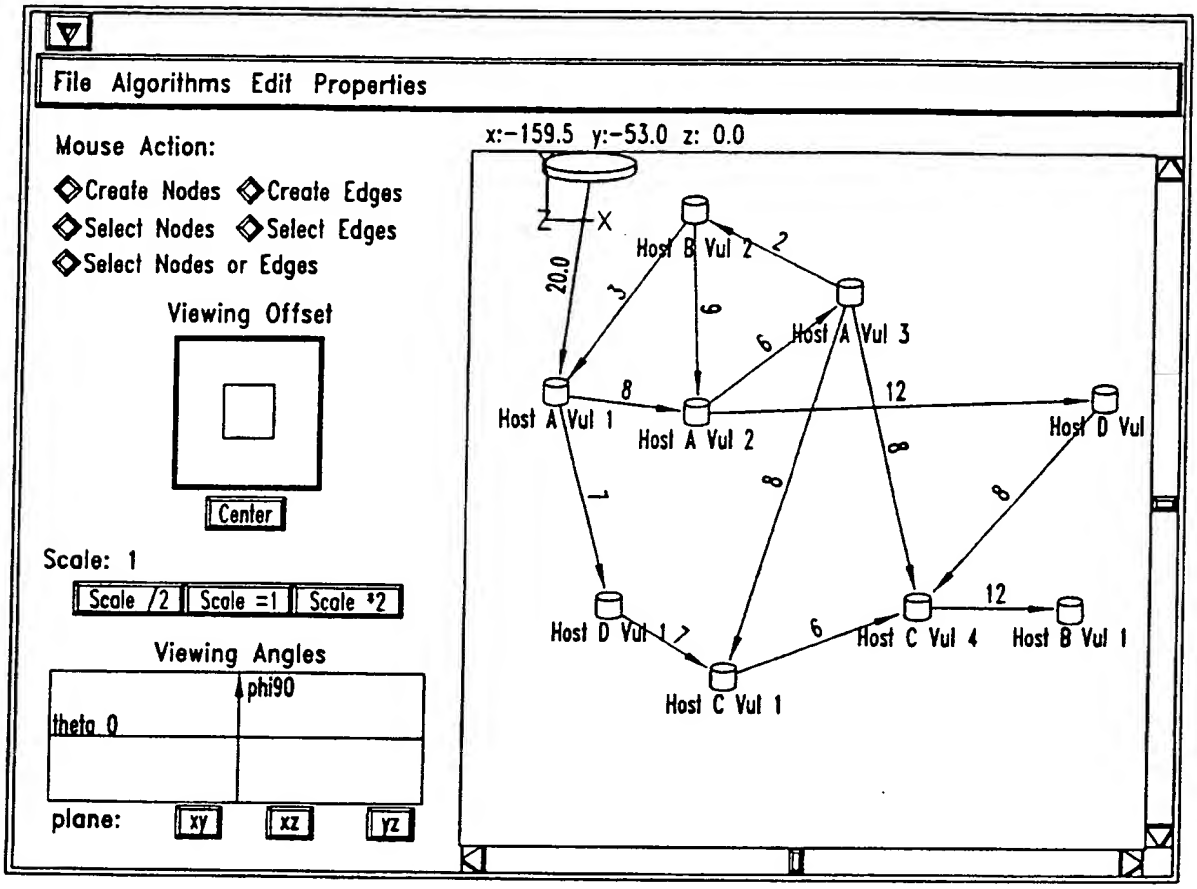

File Algorithms Edit Properties
Mouse Action:
Create Nodes
Create Edges
Select Nodes
Select Edges
Select Nodes or Edges
Viewing Offset
Center
Scale: 1
Scale /2
Scale =1
Scale *2
Viewing Angles
phi90
theta 0
plane:
xy
xz
yz
x:-159.5 y:-53.0 z: 0.0
Host B Vul 2
Host A Vul 3
Host A Vul 1
Host A Vul 2
Host D Vul
Host D Vul 1
Host C Vul 4
Host B Vul 1
Host C Vul 1
20.0
2
3
6
6
8
12
1
8
8
8
7
6
12

FIG. 20

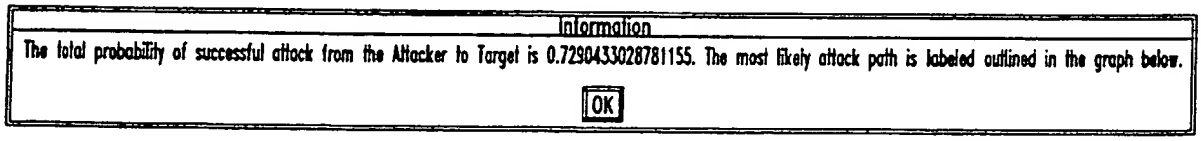

Information
The total probability of successful attack from the Attacker to Target is 0.7290433028781155. The most likely attack path is labeled outlined in the graph below.
OK

FIG. 21

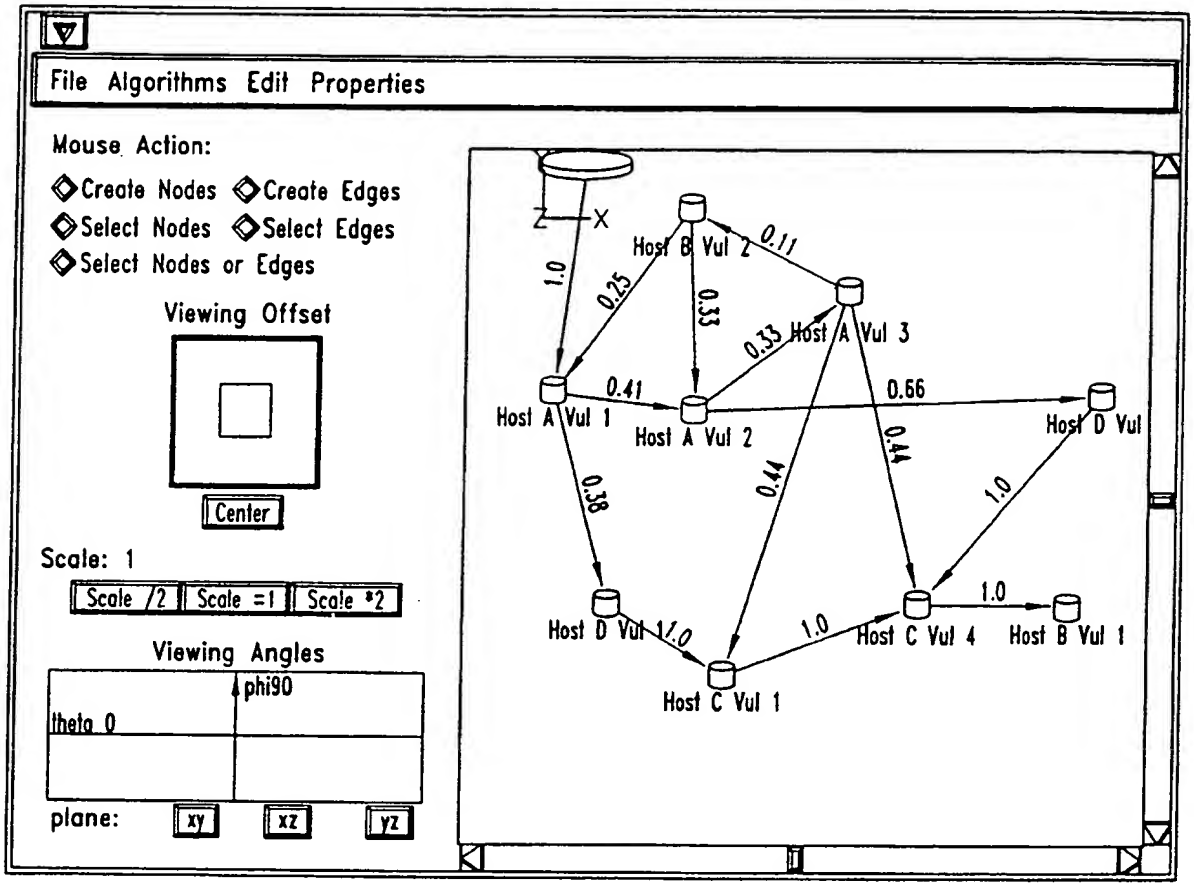

File Algorithms Edit Properties
Mouse Action:
Create Nodes
Create Edges
Select Nodes
Select Edges
Select Nodes or Edges
Viewing Offset
Center
Scale: 1
Scale /2
Scale =1
Scale *2
Viewing Angles
phi90
theta 0
plane:
xy
xz
yz
Z
X
Host B Vul 2
Host A Vul 3
Host A Vul 1
Host A Vul 2
Host D Vul
Host D Vul 1
Host C Vul 4
Host B Vul 1
Host C Vul 1
1.0
0.25
0.33
0.11
0.33
0.41
0.66
0.38
0.44
0.44
1.0
1.0
1.0
1.0

FIG. 22

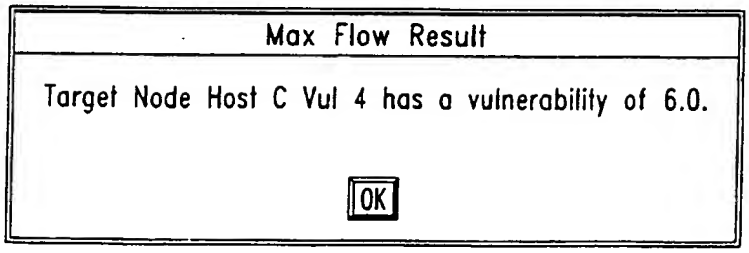

Max Flow Result
Target Node Host C Vul 4 has a vulnerability of 6.0.
OK

FIG. 23

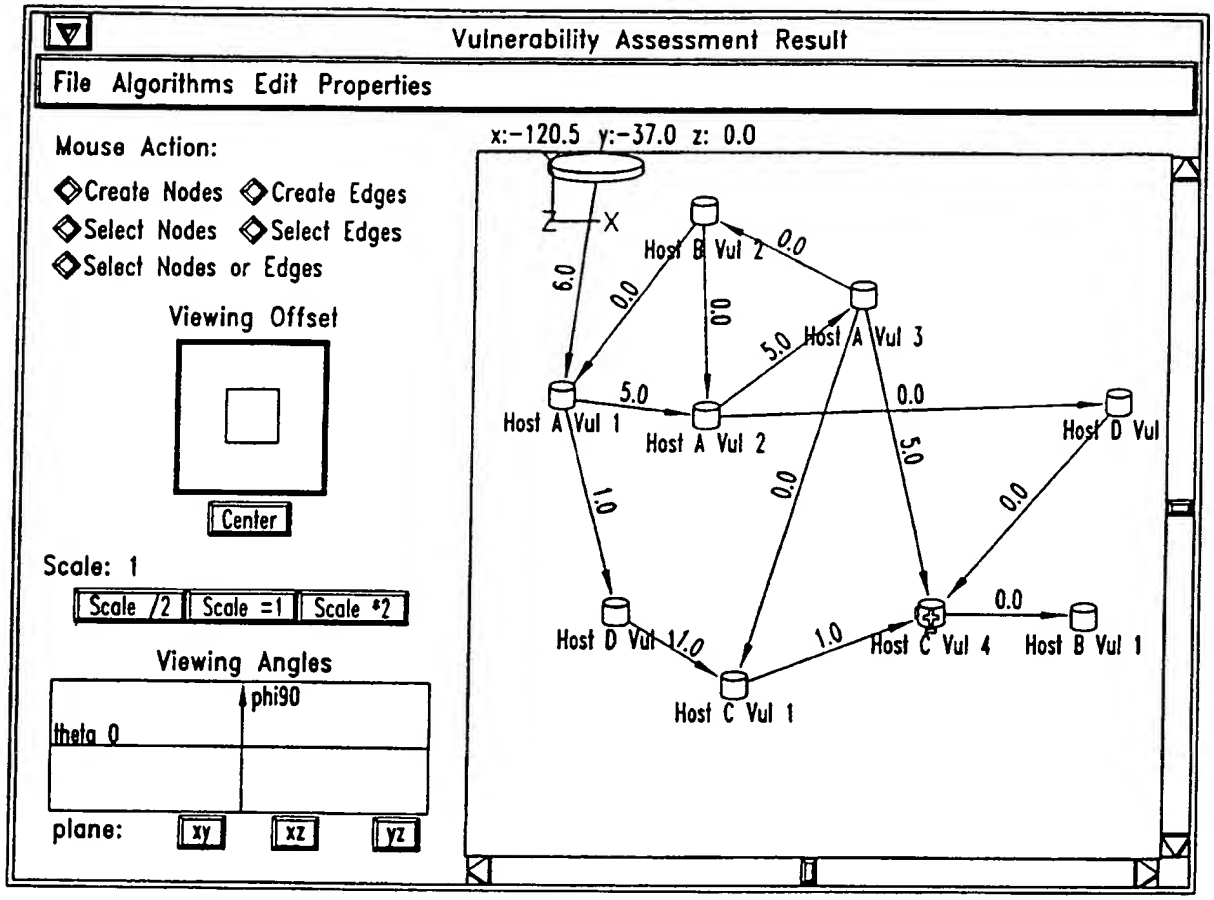

Vulnerability Assessment Result
File Algorithms Edit Properties
Mouse Action:
Create Nodes
Create Edges
Select Nodes
Select Edges
Select Nodes or Edges
Viewing Offset
Center
Scale: 1
Scale /2
Scale =1
Scale *2
Viewing Angles
phi90
theta 0
plane:
xy
xz
yz
x:-120.5 y:-37.0 z: 0.0
Host B Vul 2
Host A Vul 3
Host A Vul 1
Host A Vul 2
Host D Vul
Host D Vul
Host C Vul 4
Host B Vul 1
Host C Vul 1

FIG. 24

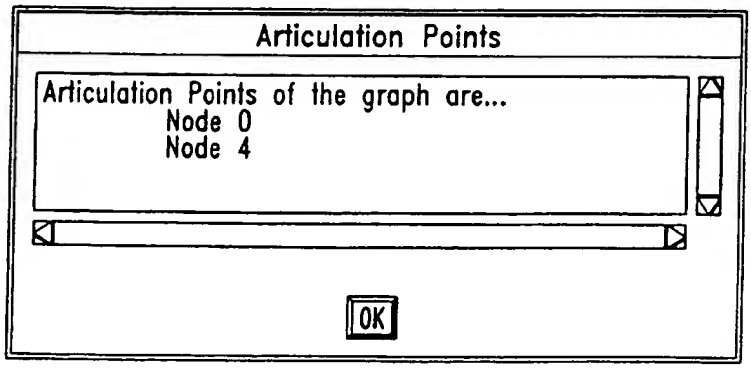

Articulation Points
Articulation Points of the graph are...
Node 0
Node 4
OK

FIG. 25

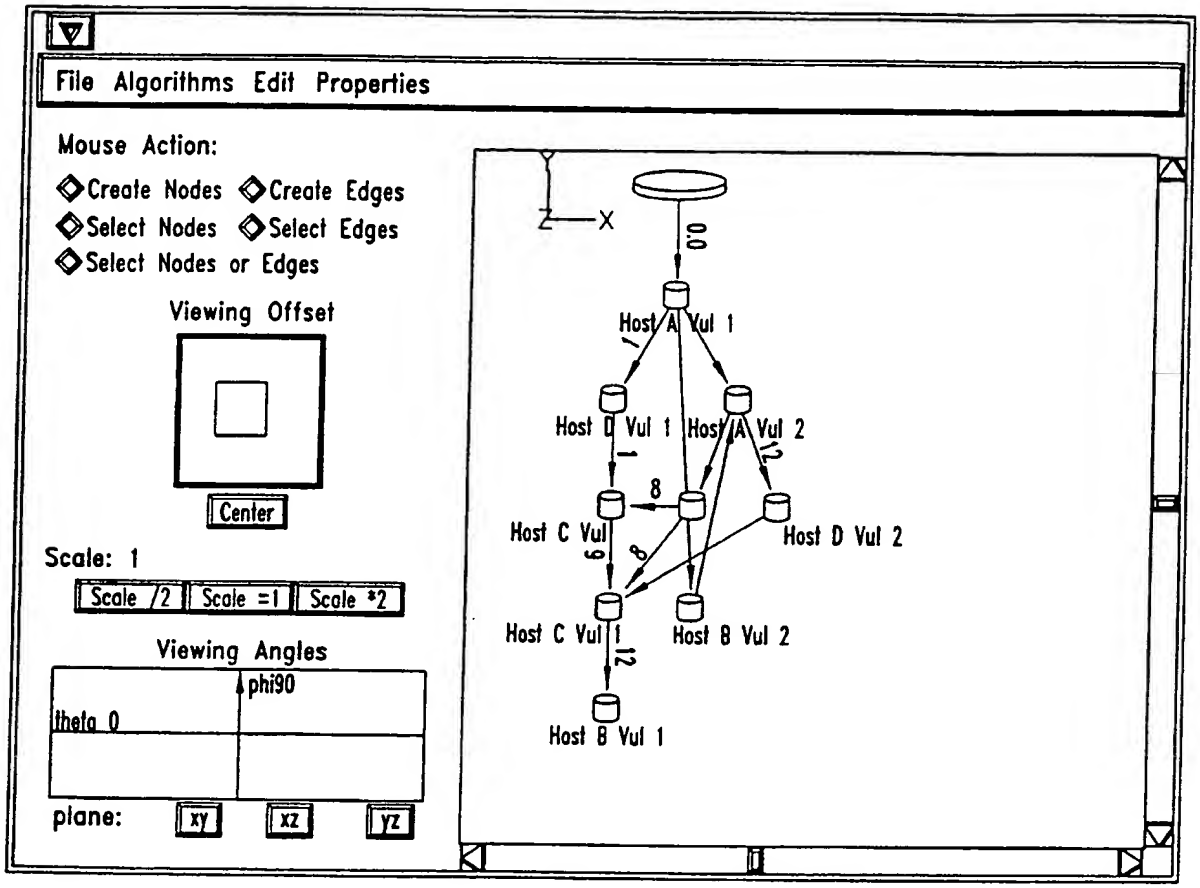

File Algorithms Edit Properties
Mouse Action:
Create Nodes
Create Edges
Select Nodes
Select Edges
Select Nodes or Edges
Viewing Offset
Center
Scale: 1
Scale /2
Scale =1
Scale *2
Viewing Angles
phi90
theta 0
plane:
xy
xz
yz
Z
X
0.0
Host A Vul 1
Host D Vul 1
Host A Vul 2
Host C Vul
Host D Vul 2
Host C Vul 1
Host B Vul 2
Host B Vul 1

FIG. 26

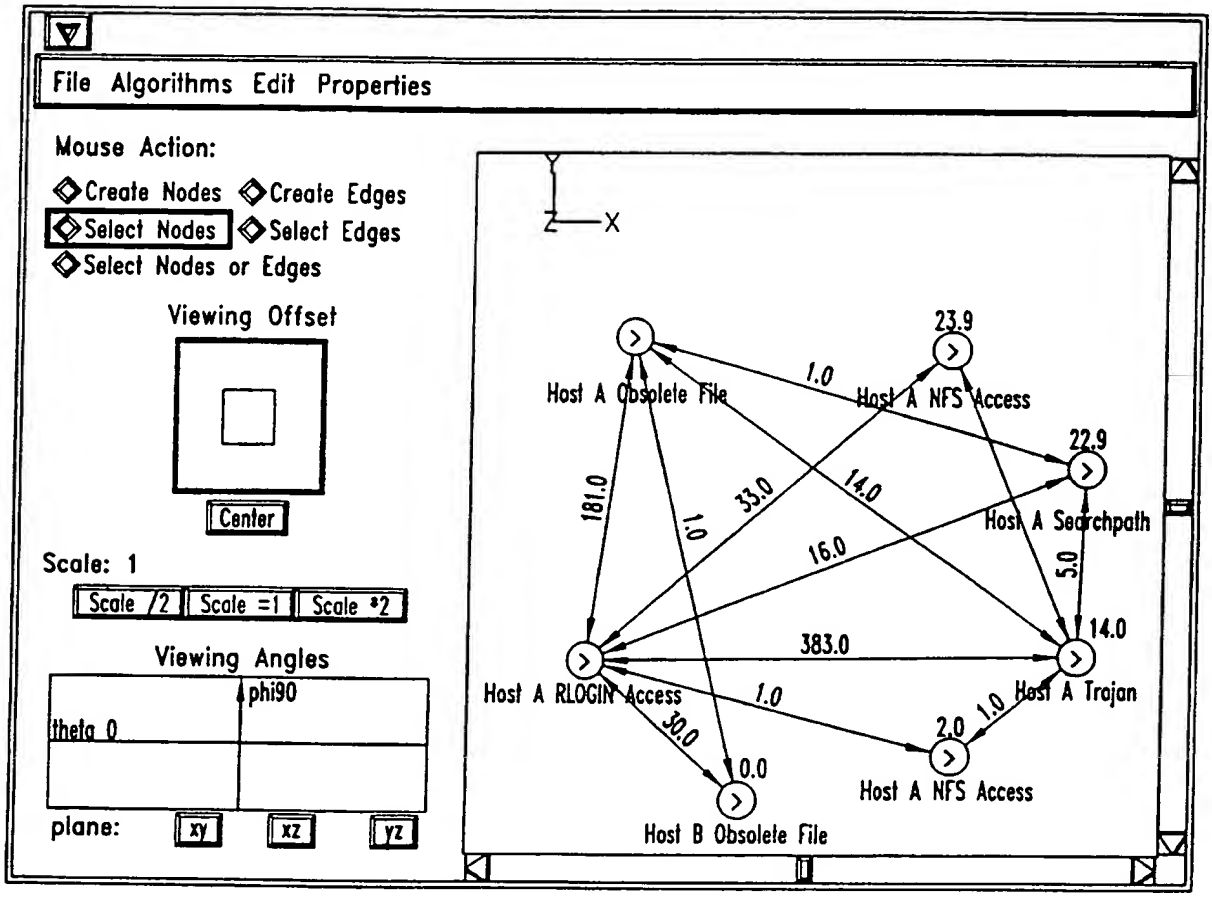

File Algorithms Edit Properties
Mouse Action:
Create Nodes
Create Edges
Select Nodes
Select Edges
Select Nodes or Edges
Viewing Offset
Center
Scale: 1
Scale /2
Scale =1
Scale *2
Viewing Angles
phi90
theta 0
plane:
xy
xz
yz
Z
X
Host A Obsolete File
Host A NFS Access
Host A Searchpath
Host A RLOGIN Access
Host A Trojan
Host A NFS Access
Host B Obsolete File
23.9
22.9
14.0
2.0
0.0
1.0
181.0
33.0
14.0
16.0
5.0
383.0
30.0

FIG. 27

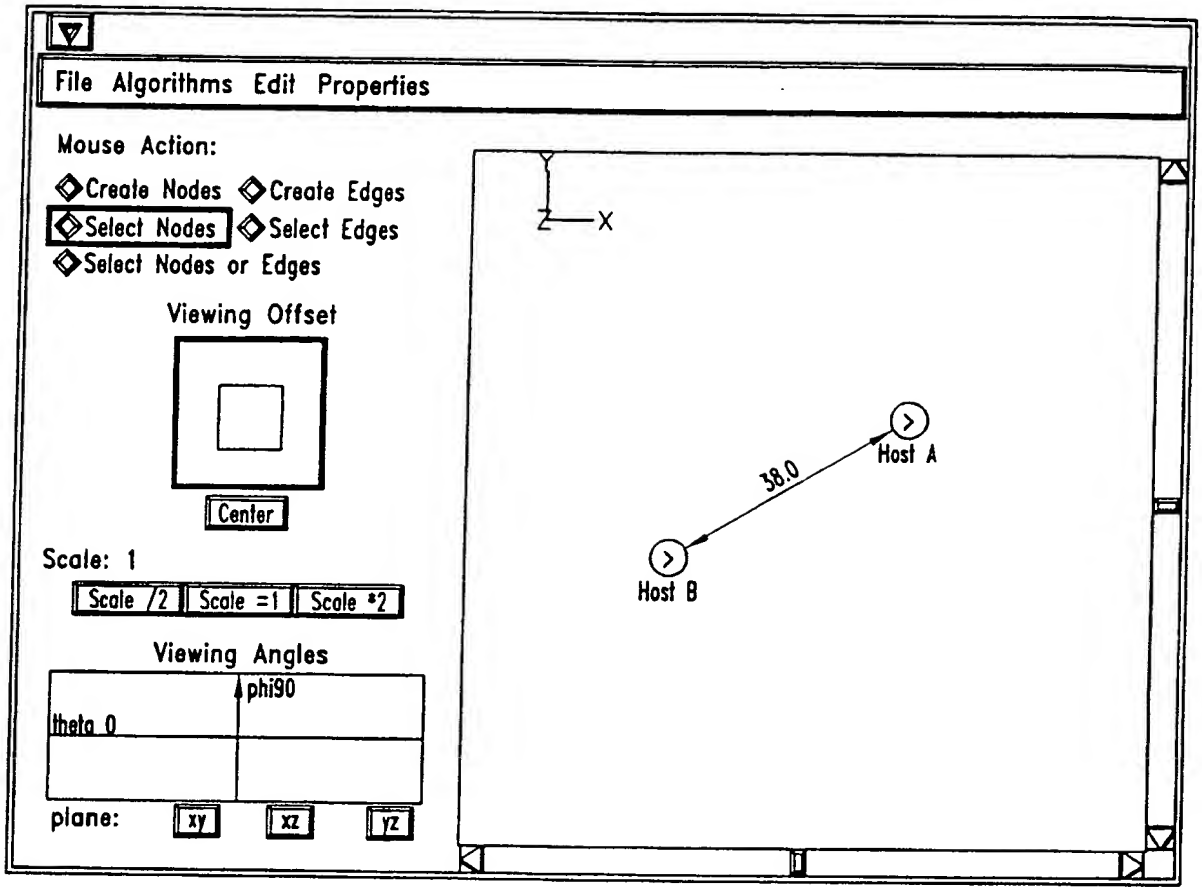

File Algorithms Edit Properties
Mouse Action:
Create Nodes
Create Edges
Select Nodes
Select Edges
Select Nodes or Edges
Viewing Offset
Center
Scale: 1
Scale /2
Scale =1
Scale *2
Viewing Angles
phi90
theta 0
plane:
xy
xz
yz
Z
X
38.0
Host A
Host B

FIG. 28

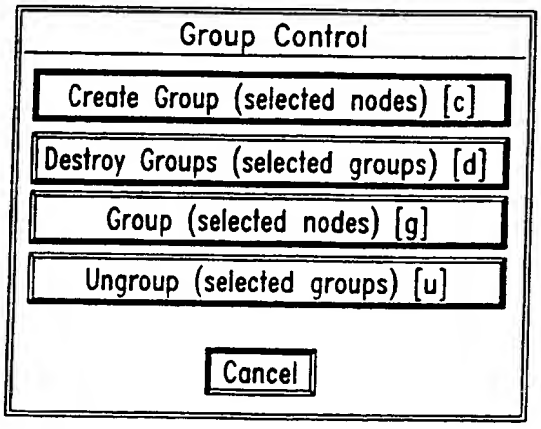

Group Control
Create Group (selected nodes) [c]
Destroy Groups (selected groups) [d]
Group (selected nodes) [g]
Ungroup (selected groups) [u]
Cancel

FIG. 29

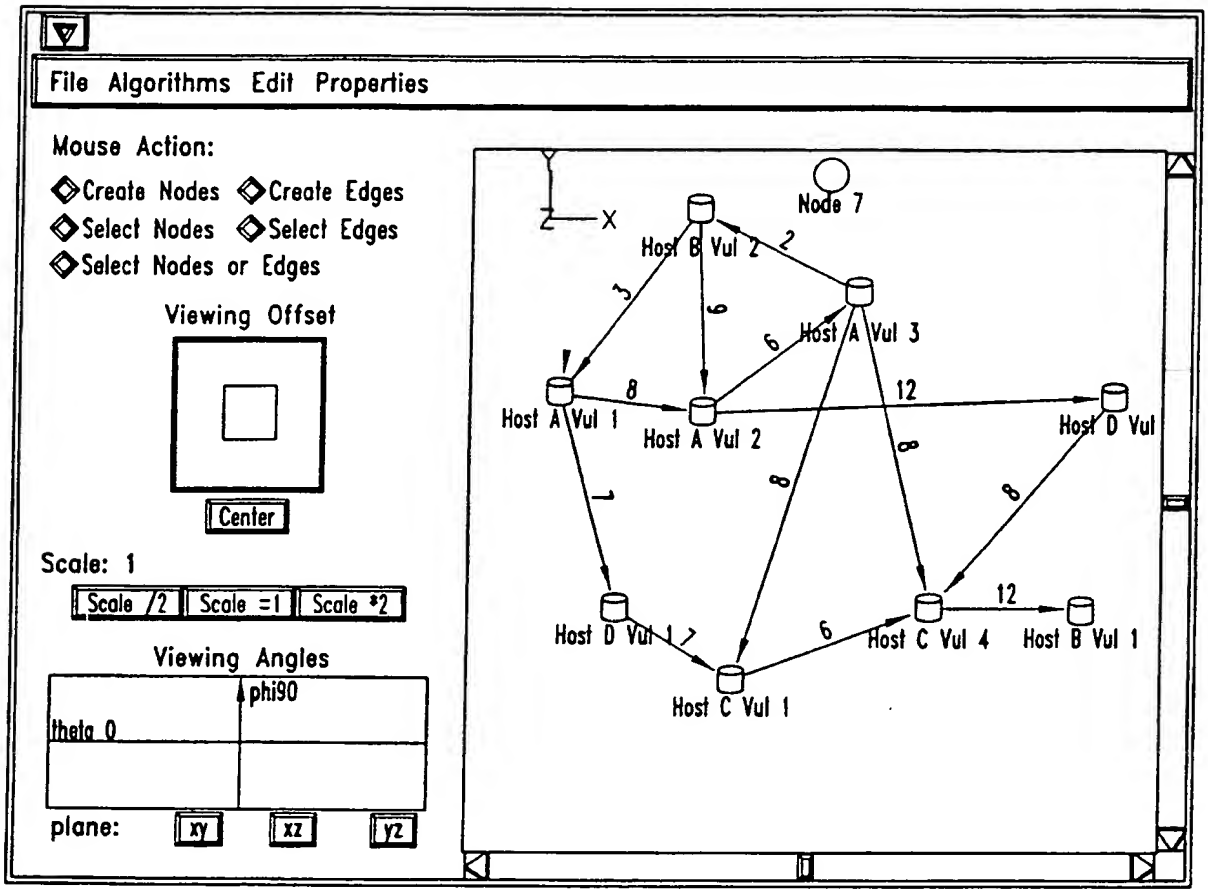

File Algorithms Edit Properties
Mouse Action:
Create Nodes
Create Edges
Select Nodes
Select Edges
Select Nodes or Edges
Viewing Offset
Center
Scale: 1
Scale /2
Scale =1
Scale *2
Viewing Angles
phi90
theta 0
plane:
xy
xz
yz
Z
X
Node 7
Host B Vul 2
Host A Vul 3
Host A Vul 1
Host A Vul 2
Host D Vul
Host D Vul 1
Host C Vul 4
Host B Vul 1
Host C Vul 1
2
3
6
6
1
8
12
7
8
8
8
12
7
6

FIG. 30

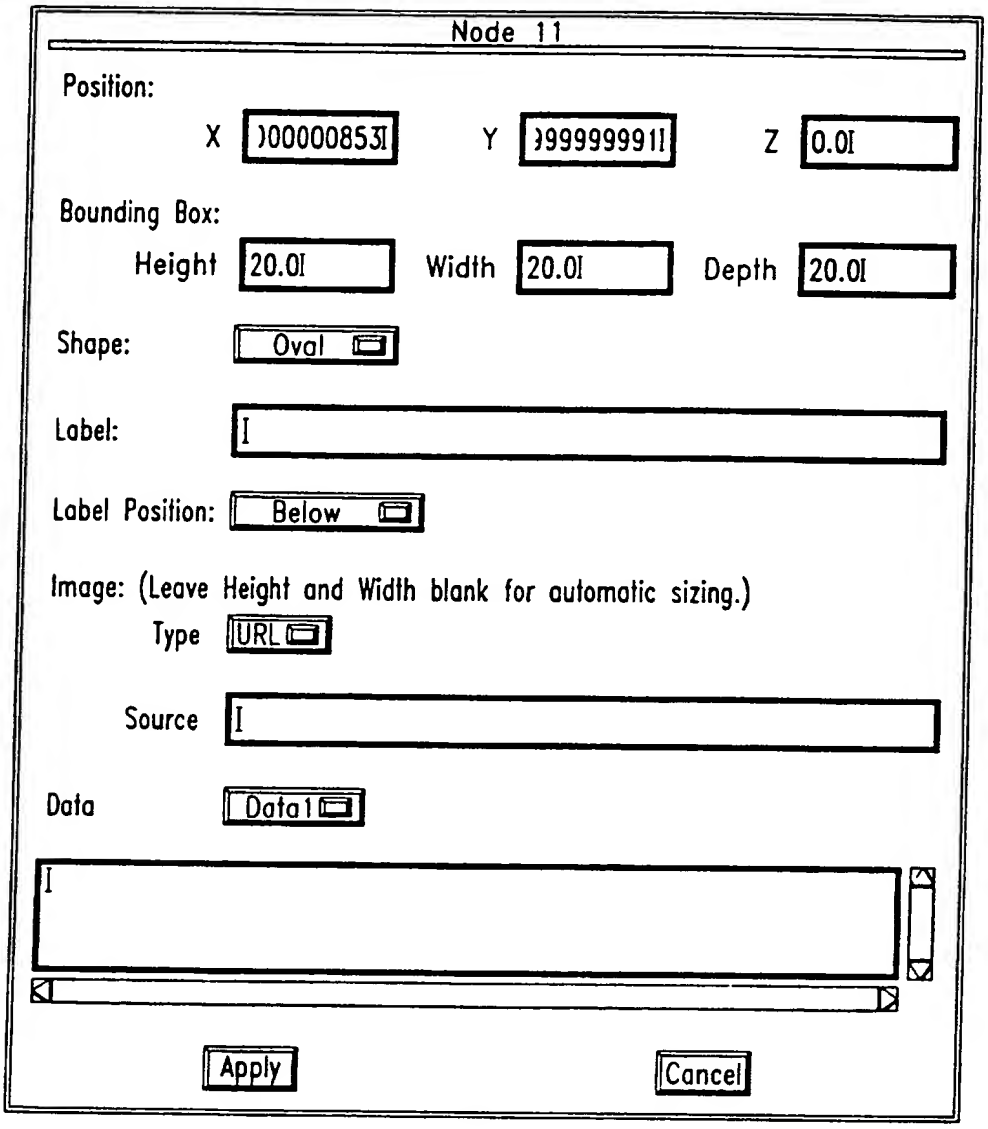

Node 11
Position:
X
Y
Z
0.0I
Bounding Box:
Height
20.0I
Width
20.0I
Depth
20.0I
Shape:
Oval
Label:
Label Position:
Below
Image: (Leave Height and Width blank for automatic sizing.)
Type
URL
Source
Data
Data1
Apply
Cancel

FIG. 31

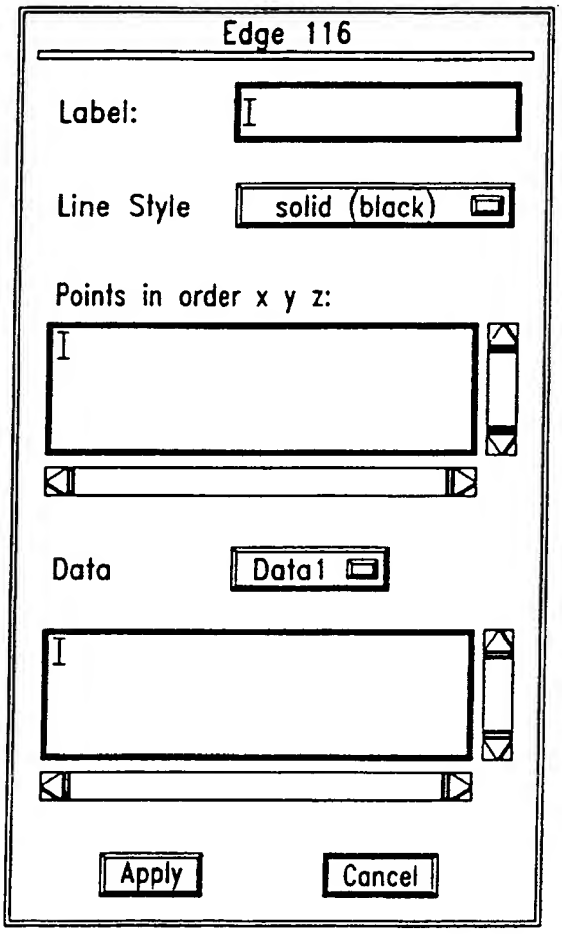

Edge 116
Label:
Line Style
solid (black)
Points in order x y z:
Data
Data1
Apply
Cancel

FIG. 32

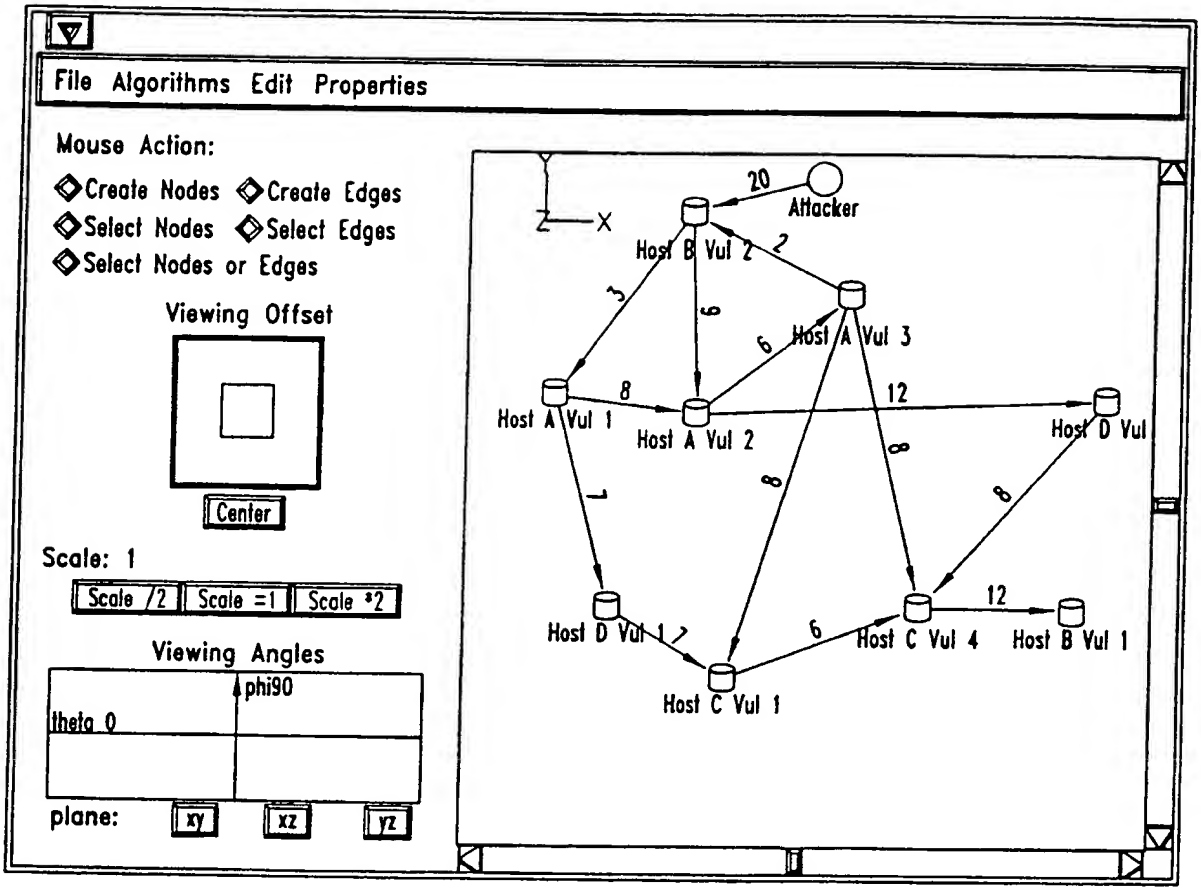

File Algorithms Edit Properties
Mouse Action:
Create Nodes
Create Edges
Select Nodes
Select Edges
Select Nodes or Edges
Viewing Offset
Center
Scale: 1
Scale /2
Scale =1
Scale *2
Viewing Angles
phi90
theta 0
plane:
xy
xz
yz
Attacker
20
Host B Vul 2
2
3
6
6
Host A Vul 3
8
12
Host A Vul 1
Host A Vul 2
Host D Vul
1
8
8
8
Host D Vul 1
7
6
12
Host C Vul 4
Host B Vul 1
Host C Vul 1

FIG. 33

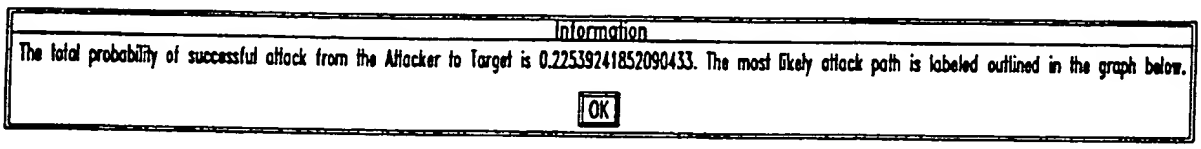

Information
The total probability of successful attack from the Attacker to Target is 0.22539241852090433. The most likely attack path is labeled outlined in the graph below.
OK

FIG. 34

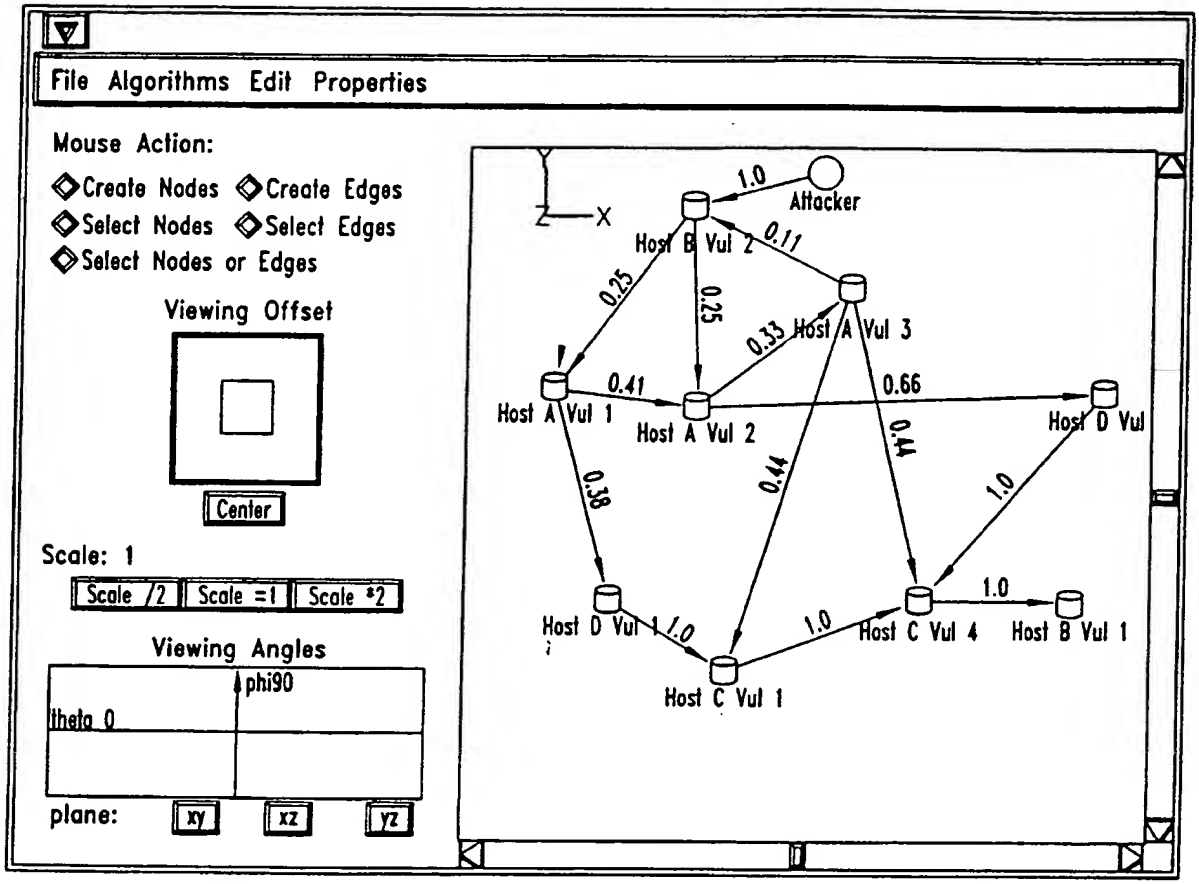

File Algorithms Edit Properties
Mouse Action:
Create Nodes
Create Edges
Select Nodes
Select Edges
Select Nodes or Edges
Viewing Offset
Center
Scale: 1
Scale /2
Scale =1
Scale *2
Viewing Angles
phi90
theta 0
plane:
xy
xz
yz
Attacker
Host B Vul 2
Host A Vul 3
Host A Vul 1
Host A Vul 2
Host D Vul
Host D Vul 1
Host C Vul 4
Host B Vul 1
Host C Vul 1
1.0
0.11
0.25
0.25
0.33
0.41
0.66
0.44
0.38
0.44
1.0
1.0
1.0
1.0

FIG. 35

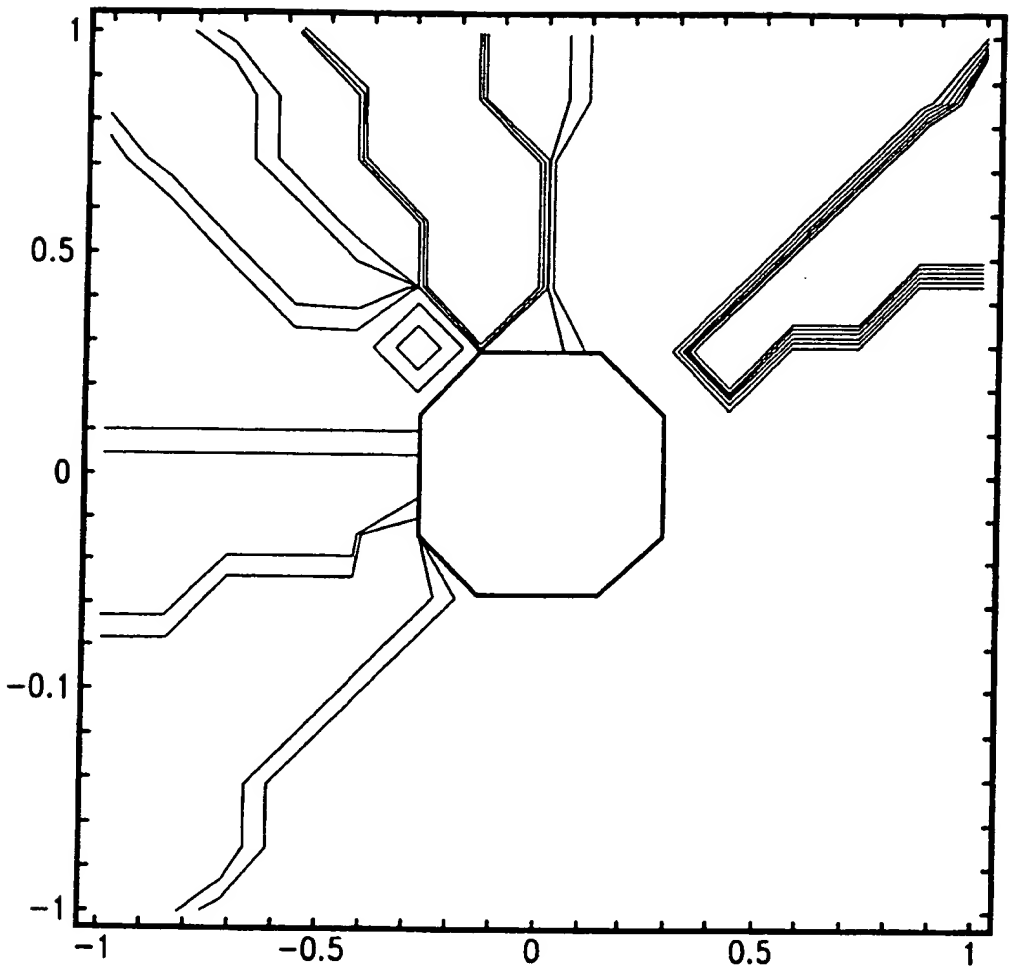


FIG. 36

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/12724

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : G06F 11/30
US CL : 713/201
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/201, 210; 714/1, 14; 345/440

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST
search terms: vulnerable, vulnerability, normalized, graph

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,892,903 A (KLAUS) 06 April 1999, All	1-18
Y	US 5,485,409 A (GUPTA et al) 16 January 1996, All	1-18
Y	US 5,684,957 A (KONDO et al) 04 November 1997, All	3, 4, 6, 10, 11, 16
A,E	US 6,088,804 A (HILL et al) 11 July 2000, All	
A,E	US 6,089,456 A (WALSH et al) 18 July 2000, ALL	

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 04 AUGUST 2000	Date of mailing of the international search report 24 AUG 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer ROBERT W BEAUSOLIEL JR Telephone No (703) 308-7090

Eugenia Zogan

Form PCT/ISA/210 (second sheet) (July 1998)*